Blacklisted 411

The Official Hackers Magazine

Hack The System...

Current News

DEFCON 14 was a Success
BL411 Looking for New Writers
2007 Membership Card Design Finished

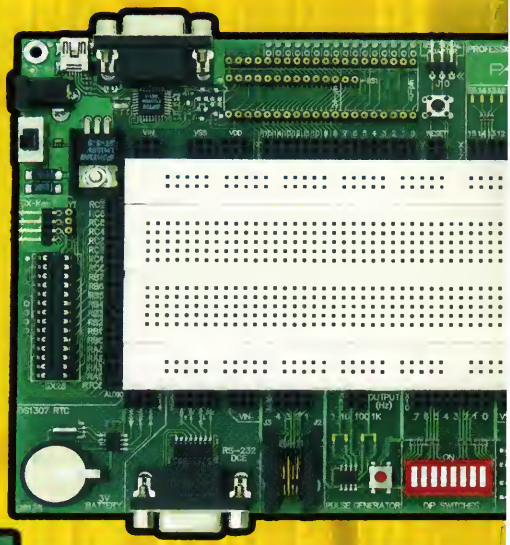
Inside This Edition

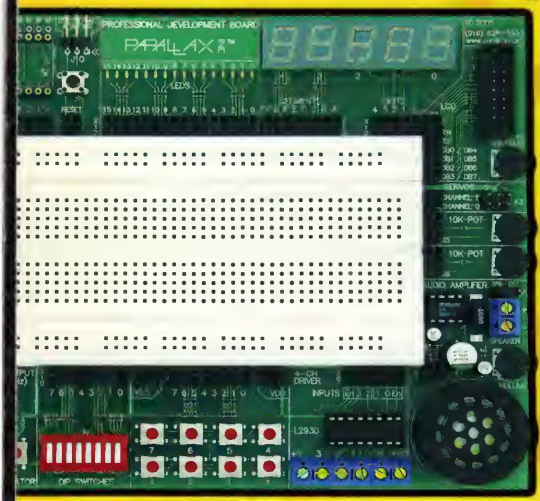
VOLUME 8 ISSUE 3 FALL 2006

A Solderless Microcontroller Evaluation Board

Increase your hardware foo

Never fear hardware again with the **Parallax Professional Development Board (PDB). A variety of typical I/O (LEDs, LCD interface, buttons, etc.) devices and circuitry are built into the PDB,** providing users with an **ideal experimentation environment for microcontroller projects.** Three sets of sockets are provided that allow the board to accommodate the BASIC Stamp 1 module, the 24- or 40-pin BASIC Stamp-style modules, the 24-pin Javelin Stamp module, and the SX28AC/DP Microcontroller with an SX-Key. **Order Parallax part #28138.**





Features include:

- Parallel port for LCD
- Pulse generator
- L293D high-current driver
- Audio amplifier
- DS1307 Real-Time clock
- (8) push buttons
- (8) DIP switches
- (2) 10K potentiometers
- RJ-11 port
- (16) blue LEDs
- (5) 7-segment LEDs
- (2) servo headers
- Power supply switch

$149

PARALLAX INC

www.parallax.com

Be sure to check out the LosT-Neural TCP/IP contest at DC14!

Blacklisted! 411 staff & contributors

Editor in Chief
Zachary Blackstone

Assistant Editors
Alexander Tolstoy
Dave S.

Office Help
Pixel Pixie, Jess, Lexus, Dark Paladin, DoctorWHO, MomoPi, Mr. Asshole

Artwork
Derek Chatwood - A.K.A. Searcher
Kate O., Parallax, Mason/Wolf

Distribution
Greg, Boiler, Syntax, David B.

Photography
CHS, Dark Paladin, Daniel Spisak

Web Admin
Ustler

Writers
Ustler, Unicoder, Dr. Fibes, Jeremy Martin, The Goldfinger, dual_parallel, MobbyG, Cactus Jack, ML Shannon, Grandpa Hackman, Electra-Solve

Inside this issue

Additional information

Subscriptions:
$20 U.S., $24 Canada, $35 Foreign
Check or Money Order (U.S. Funds only)

Letters/Articles:
Blacklisted! 411 Letters and Articles
P.O. Box 2506, Cypress, CA 90630
(Include name & address—we PAY for articles)

Advertising:
Blacklisted! 411 Advertising
P.O. Box 2506, Cypress, CA 90630
Email: advertising@blacklisted411.net

World Wide Web:

Website: http://www.blacklisted411.net
Store: http://store.blacklisted411.net
Forums: http://www.bl411forums.com

ISSN 1082-2216

9035768ABBAJBVJB-0027

DBBL 01,07,32,41,52

PRINTED IN THE UNITED STATES OF AMERICA

Icons used on the front cover are from Dropline Neu! created by Silvestre Herrere and are released under the GNU General Public License (GPL). A full copy of the license and icons can be located at http://www.silvestre.com.ar/or available on request as required.

Blacklisted! 411 introduction for those of you who are new…..

Who we are… and were…

The question often arises on the subject of, "How did it all start?" in reference to our magazine and it's history. In response to this popular question, here is a quick history lesson of *Blacklisted! 411* magazine, including names, dates and little known facts which have, thus far, been hidden away for years…

Blacklisted 411 magazine dates back to October 1983 with a group of friends from a Southern California high school that shared a common interest. They were all deeply interested in their Atari, Apple and Commodore computers, electronics, sciences, arcade games, etc. They built projects, hacked into various things, made their own programs, came up with grand ideas and tried to make them into some sort of reality. The group started a monthly hackers "disk magazine" (an early form of what is now known as an e-zine) called "*Blacklisted 411, The hackers monthly*". This may sound strange today but circulating information on disk was the best way to get it out (at the time) without all the cool toys we take for granted today. There was no internet to utilize and nobody had printers which could print anything other than plain text (and didn't even do that well). With a disk based system, text files, primitive graphics/pictures, and utilities were fairly easy to distribute and it could be copied by anyone who had a compatible computer. At our peak, at least 150 disk copies <per month> of the disk magazine were sent into the public, though there is no way to know how many were copied by others.

Eventually modems caught on and the magazine was distributed through crude BBS systems. Using the power of a Commodore 64, a *Blacklisted! 411* info site, which anyone could log into without handle or password, was created and operated. It was a completely open message center. Using X-modem or Punter file transfer protocols, one could download the latest *Blacklisted! 411* files or read/leave "messages" which later became known as a "message base" and has evolved into what are now commonly known as "newsgroup postings" or "forum postings". There was only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984, the purchase of a 9 pin dot matrix printer that could <gasp> print basic graphics was entered into the mix. Printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school became the new "experiment". The media center staff graciously allowed the production of these copies free of charge which was very cool at the time. The copies were passed out at the local "copy meets" (an interesting phenomenon of past times - hordes of computer users would meet at a predetermined location and setup their computers with the sole purpose of copying software and exchanging this software with each other). Piles of the magazine were left anywhere and everywhere people could see them. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. It's been a longtime myth that people photocopied those original copies and then those were photocopied, etc. There's no telling just how many generations of early printouts of *Blacklisted! 411 monthly* made it out there.

Years went by and *Blacklisted! 411* evolved. The short life-span of the printouts was both a great success and a miserable failure. No matter where they were left, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but the inability to meet this growing demand was completely overlooked. The plug was officially pulled on the printout experiment and distribution through diskettes remained the norm. It was really the easiest way to go at the time. The *Blacklisted! 411* info site grew into a 2-line system. This was a big deal in 1985. By that time, information was almost exclusively passed around by modem (unofficially on paper) and disks were still being released at this time.

June of 1987 marked the end of *Blacklisted! 411, The hackers monthly*. The last disk based magazine (# 46) was distributed that month. Since all of the original crew were finally out of high school and onto college, work and the bigger/better things in life, nobody had the time or inclination to put any effort into the disk based magazine anymore. The once thriving *Blacklisted! 411* group broke up and people went their separate ways. Naturally, it was assumed that this was the end and *Blacklisted! 411* would never be resurrected in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zachary Blackstone, felt it was time to revive the *Blacklisted! 411* concept, but this time do it as a print magazine. It was extremely difficult to get started because the group was no more and he was alone. He was the only one of the original group members remaining that had an interest in bringing the hacker group and magazine alive again. With some money, the will to make it happen, top of the line (at the time) computer gear and page layout software, *Blacklisted! 411* was reborn. *Blacklisted! 411* Volume 1, Issue 1 was released in January 1994. *Blacklisted! 411* was finally BACK. The issues were released monthly and distribution was small. Regardless, the related user meets were packed! The interest in the magazine was great. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zachary managed to get in contact with many of the old group members, most of whom which are active staff members even today.

In 1999, what was to be the last issue of *Blacklisted! 411* (Volume 5, Issue 4) was published. It was unknown at the time, but many pitfalls would ultimately cause the demise of the magazine. Officially, it was dead as a doornail. After 4 years of regrouping and planning, *Blacklisted! 411* magazine was resurrected yet again..

To date, Blacklisted! 411 is one of the oldest group of hackers still remaining and releasing gathered and compiled information within the hacker community and the mainstream community as well. Hanging onto the very same hacker mentality and code of ethics from the 80's, Blacklisted! 411 stands apart from the rest. Their ideal is that hackers are not thieves - they're curious people who are the makers and shakers of the technology sector. They're not elitist hackers by any means and believe that no question is ever a "stupid" question. Old school hackers and newbie hackers alike, Blacklisted! 411 caters to you.

What' about now…

Community

The last two years have been an exciting time for the staff and crew over here. We have become extremely active in the hacker community. As we are based in the Los Angeles area, we have built relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and many others. We have been attending and sponsoring Hacker Conventions and Conferences such as the Layer One Convention and the ever popular Defcon. You can find us attending these conventions regularly. We usually run a vendor booth at these events and we make available our wares - subscriptions, back issues, t-shirts, hats, stickers and other SWAG. We also provide several "convention only" promotions such as the Apple IPOD give-away we held at DefCon 13. Our give-away was a big hit. We're planning on attending DefCon 14 this year and we'll be holding our own private catered reception for subscribers and supporters. Additionally, we'll be handing out membership cards with all new subscriptions this year. Whatever you do, be sure to check out our booth first, you'll be glad you did!

Magazine Development
A major effort has been made to increase our exposure to the hacking and information security community. Our distribution goals for the magazine was to break 100K copies distributed each quarter sometime in 2004 and we far surpassed our goal within our timeframe.. To date, Blacklisted! 411 has a circulation over 200,000 copies per issue. Based on orders from distributors and sell through, we're doing excellent in the marketplace. Additionally, we have been seeking and hiring freelance writers, techs, photographers, and editors to increase the quality and scope of the magazine. We've also been promoting the magazine outside of our community to bring in cross-over readers.

Merchandising / SWAG
We now have a whole series of *Blacklisted! 411* themed swag and merchandise. This currently includes stickers and apparel, but will soon include posters, a new DVD, gadgets and technology.....whatever our creative minds can come up with. Ideas and suggestions on this subject will be accepted and appreciated.

Charities
People generally believe that hackers are awful scum-sucking low life degenerates not fit to inhale the air they breathe. This idea has been pounded into the heads of people repeatedly by the mainstream media. Not necessarily because they're evil-doers, but more likely due to the fact that they simply have no idea what hackers are or what we're all about.

They think we're an uncaring bunch of thieves. They couldn't be any further from the truth. Hackers do care. In fact, they probably care more about the things that really matter than your average Joe does.

Blacklisted! 411 is owned and operated by real people who care about things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community by offering real support, not only have we done a good deed, but we've demonstrated our philosophy at it's core level. We want to help. As such, *Blacklisted! 411* Magazine has officially donated to several local charities in an effort to achieve this goal.

First and foremost is the local chapter of the Ronald McDonald House. Many people have never even heard of this place, but nevertheless, they're a wonderful bunch of people who offer an amazing service to those less fortunate families who have a child in the hospital....they offer a place to stay and a hot meal - for FREE (or a very small donation if you can afford it). We've donated many items to help their cause because we really believe in it. One of our favorite donations was the 200 some odd small children costumes we supplied them with to give to the children around Halloween. If you have children of your own, maybe you can appreciate this place a little better. *Blacklisted! 411* Magazine wholeheartedly supports the Ronald McDonald House mission and their programs.

Additionally, we've donated heavily to the Westminster Parish Festival, specifically with the intent to help support their youth programs and special classes for the mentally and physically handicapped. The festival they operate is much like a small carnival with rides, food, drinks, and entertainment. They also run a huge raffle which is right up our alley as far as lending a helping hand goes. We've been able to supply them with some unique and stunning prizes for the children who attend the festival. Prizes you wouldn't expect to win for a cheap raffle ticket.

Our hope is that we were able to brighten up the day for some children, maybe even a family or two....and help our community at the same time.

Of course, we also donate to EFF and other hacker-friendly groups. That really goes without saying, right?

Closing thoughts
Let's start our closing thoughts by mentioning that we're your friendly neighborhood hacker magazine. We're one of the team players and happy to help people. Please don't feel that you cannot approach us.

So, if you have questions, comments, articles, ideas, suggestions, have a business proposition or wish to offer support in some way, please contact us and let's see what we can come up with. Thanks for your support, hackers!

BL411

Important notes of interest:

SWAG NOW AVAILABLE

That's right! We have SWAG now. We have some cool "Hack the System" T-shirts and baseball caps, plus a wide variety of bumper stickers available at our online store. We'll soon have some additional SWAG and technology available as well. Keep watching. www.blacklisted411.net

DEADLINES

For some reason, people seem to miss our deadline mention in the magazine and online, so be sure to read this. The DEADLINE for articles, letters, artwork and ads for Volume 8, Issue 4 is January 21st, 2007. Got that? JAN 21 2007

ADVERTISING

People often email us asking if classifieds are free. We keep telling everyone YES. Classifieds are free. If you have a classified you want us to run and it's topic related to the magazine, send it in and we'll consider it. Ads are limited to space constraints per issue. First come, first served. Naturally, we reserve the right to reject advertising for any reason.

ARTICLES

Do we really need to mention this one? We're a magazine and we NEED articles. If you're a writer and want us to consider your work, send something to us. Don't waste any time. We're a PAYING MARKET. What does that mean? It means that we pay for articles which we use...but only if you want the $. We can donate your payment to your favorite charity if you'd like. Our rates are generally $25 a page, depending on size, quality & use of photos.

ONLINE CONTENT

If you haven't noticed it yet, we have a website (www.blacklisted411.net) and we like to fill our pages with interesting, topic related content. If you'd like to write articles/reviews for use on our website, send them in.

Letter from Zachary Blackstone, editor-in-chief…..

Welcome to the latest edition of Blacklisted 411 Magazine. We've got some ground to cover, so I'm going to dive right on in and get to it.

As you may have noticed, this issue has been released relatively early considering the Summer issue's late release. We're trying to close the gap on our issues for 2006 so we can actually release four issues this year.

After the super-late release of Volume 8 Issue 2, people began to ask if we were going to just skip an issue this year. Looking back at my letter from the editor from the Summer edition, it's obvious that my coverage of this topic was inadequate. The short of it is that we're going to try and squeeze out four entire issues this year, even if it means the time between the last few issues is shortened.

Additionally, some readers were worried that they were going to be stiffed an issue. I'd like to make this one crystal clear to everyone. If you paid for a subscription, you'll receive the number of issues you paid for (ie: 4 issues for a 1yr subscription, 8 issues for a 2yr subscription, etc). The point is that we consider a years worth of subscriptions to be four issues. This is how we determine that a subscriber gets what they paid for. I hope this clears things up for everyone.

Another complaint is that we don't communicate with our readers as well as we could. We've already put changes in place to alleviate this issue. Not only are we posting regular updates to the main page of our website, but we're leaving those messages there a little bit longer and storing them in our news section database so they can be viewed even when they're not on the main page any longer. In the past, we would delete various news items from time to time, mainly due to a technical issue we tried to get around. We no longer delete our news items. I believe that these changes will correct any general communication issues we've been having.

About the page count of the magazine. Ever since the day the magazine was made available to the public, it was a 60-page "digest" format. We decided to try something new somewhat recently. Volume 7 Issue 4 and Volume 8 Issue 1 were both released as 84-page "digest" format. We added 24 pages of extra content in each of those two issues. We didn't increase our cover price or increase our subscription prices. However, our handling cost was increased dramatically. The weight of the additional 24 pages per copy added up! We knew it would, but we were willing to eat the additional cost to try out our idea. Our hope was that the increased page count would increase sales and interest in the magazine.

While the interest did appear to increase, the sales did not. After two issues of testing out this theory, it was decided to pull the plug on the idea and revert back to our original 60-page format.

So, what have we been doing over here at the magazine lately? We've been making sweeping changes across every level of the magazine. Some of these changes are obvious while others are not easily noticed. I'll take some time now to explain some of what's going on.

First and foremost would be the forum. If you haven't noticed already, check out the forum! We migrated over to vBulletin from the phpBB platform. vBulletin will give us much more creative control of how we use our forum. We intend to use the forum to provide a reliable means for the community to share ideas and communicate with the magazine staff. If you have not done so yet, please check out the forum. By the way, if you're a subscriber, contact Alex so he can set you up with subscriber access to the forum. Be sure to include real name/address so he can identify your subscription status.

Subscriber access to the forum may not sound like much, but let me explain what this will include. First of all, subscriber access to the forum will give you immediate access to the full range of sections, including a special subscriber-only area that has a Q&A topic directly linked back to and operated by the magazine staff. Additionally, as soon as we bring the online magazine back, subscribers will have immediate access to it. We're also going to create a few other interesting items for subscribers. A radio show and possibly a TV show. It's only going to get more interesting as time passes. Stay tuned.

Note: If you're not already a subscriber, you can subscribe directly from the forum area and get instant upgraded access to the forum. Just click on the "SUBSCRIBE NOW" link near the top of the page.

Like I said, we're working on a Radio Show which is being headed up by "TheInstallGuy" and we're considering the idea of putting together a monthly (maybe even a weekly) TV Show. We don't have any specifics on either one of these yet, but we're accepting suggestions and offers of help from our readers for the time being. If you'd like to be part of either, send me an email right away at zachary@blacklisted411.net

You'll notice that Alex is being a lot more active lately, in both online and in-person matters. He's recently taken over as head of the magazine. This change means that he'll be bringing his business experience to the magazine which is good for backend operations and the overall health of the magazine. You'll be seeing him at more conventions and events, too. Be sure to swing by our booth at the various hacker cons.

Speaking of hacker cons, Defcon was an amazing event this year. It's 14th convention to date, they get better every year. Even though the event was moved to a new location this year which caused some grief, it was still an awesome social gathering. Quite frankly, it's arguably the best hacker con on the planet.

Unfortunately, I could not attend, but the magazine staff ran a booth in the vendor room and mingled with the attendees during the off hours. I've read the reports, I've heard the gossip and I've see the pictures. All in all, this was a great success for Dark Tangent and his awesome event! You can read about Defcon in this issue. Be sure to check it out.

What about me? Regardless of Alex taking over, I'll still be here working on the magazine itself and helping create new content for the website and anything else we come up with. In fact, you'll probably see me more often now that I have extra time on my hands. Having Alex take care of day to day has freed up a lot of my time that I would otherwise have spent dealing with magazine operations. I can now devote a significant portion of my attention to the magazine in more creative ways.

We're thinking about expanding our "street crew" to include more people who want to help spread the word about the magazine, attend meetings, conventions and be our eyes and ears in the community. We've already got a few good people taking on the project, but they can only do so much. If you like the magazine and want to help out in any way, you really should contact us and let us know. There's so many possibilities with the magazine and plenty of room for expansion. We've very receptive to ideas and constructive criticism, so don't be afraid to approach us.

As always, we want to hear from you, our readers. If you have any questions, comments, suggestions or complaints, speak up. Hack the system!!

- Editor

THE ART OF DSL

Written By: TheInstallGuy

Introduction

I feel this topic has been neglected lately and would like to reopen the topic for discussion. Since the release of VDSL, there have been a lot of changes in the way the service works and things that can be done to enhance your experience with it. Now, keep in mind that this article will primarily be based on A/VDSL connections in Canada. Most of the information here should be cross-platform. In the very least, this article should get you pointed in the right direction.

How It Works

I am sure most of you are aware of how ADSL works. I will only offer a summary here.. All DSL connections require an authentication (uname and pword). Once this is authorized by the SHASTA (Large servers used for nothing but authentication), an IP address is handed out by the RADIUS server. Alot of people are under the impression that the IP's are Dynamic, this is only partially true. An explanation of Radius servers is beyond the scope of this article, but feel free to Google it. Alright, so now you have an IP address and are able to browse. The last thing of mention here is to notice that it is actually the PPPoE adapter that gets the IP on your computer. When you first install the software for a DSL connection, (Pre-Windows XP. XP actually has built in software to do this) it creates a software layer connection that allows you to authenticate to the providers service. This connectoid is what actually receives the IP address from the provider. In Windows command prompt, running an "ipconfig /all" will show you two different connections, 1 for the actual physical network card and 1 for the software level connection. You will notice your actual network card will still have a 169….. Non-routable IP address and the software connectoid holds the valid IP to the network.

With the introduction on VDSL, a few things have changed. Most noticeably is the VDSL box that now sits atop of your TV. This new device not only acts as a DSL modem, but also acts as your TV receiver. The way this is accomplished is by sending multiple signals down the phone line (TV, DSL, Land Line). These signals are separated into frequency bands. Once inside the home, the land line or phone frequency is filtered off immediately. The remaining frequencies are sent to the TV box and filtered appropriately. Lastly, I would just like to point out that since the introduction of VDSL, all VDSL subscribers are receiving 17-20MB connections to there home! Most of that is required for the TV, but we will explore shifting that number in a later article.

How to Fix it

In this part of the article, I am going to discuss a few of the common and not so common errors seen in DSL connections. Although there are numerous sites that explain various error codes, most of them are very generic and don't help all that much. The trouble codes that are listed below are Windows XP generated. If you are using an older OS, then refer to the manual that came with the PPPoE software. There will be specific codes generated by that software.

Error 619 & 691: For all intensive purposes, these are the same. Incorrect uname and pword. The only other option here is to disable the Symantec Password Validator in MSConfig under the services tah if you are using Norton 2004 or later.

Error 769: This error tells you that your network card is disabled. Locate your network connections, right click the "local area connection" and select enable. You should be good to go.

*Note: This problem does misrepresent as error 678 on occasion.

Error 678: This one is a fun one. You have and endless selection of options. Basically, this error means that you either have no communication between your computer and the modem or no communication from the modem to your provider. If the lights flash on the modem (without a router) while you're trying to connect, then you can be fairly certain the problem exists at the provider level. Check all cables and connections and contact your provider. If the lights do not flash on the modem while trying to connect, then there is something that is blocking any communication to your modem. I will start with the most common fix and move to the more detailed. First, try power-cycling the modem and the computer. Next, as mentioned above, check network connections for a disabled network card. If the problem hasn't been resolved at this point, it is most likely due to software. Software firewalls and anti-virus are common culprits, especially after they run automatic updates. The easiest and most effective is to either disable them on startup from the MSConfig utility, or just uninstall them. Yes, the un-installation takes some time, but it will allow

you to configure them from scratch and hopefully not have the problem again in the future. Lastly, I would re-create the PPPoE connection. These connectoids due go corrupt sometimes and it is worth the 2 minutes to re-create it.

Routers: About the only thing that ever goes wrong with PPPoE and routers is the router drops the connection after a brief interruption in service. Routers are pretty sensitive to a loss of service. They will often not try to reconnect after a minute or so of no service. The most effective fix is to power cycle the modem first, wait 2 minutes, then power cycle the router. This will fix the issue 99.9% of the time.

Slow Speeds: This one can be a little tricky to diagnose, therefore I will stick to problems pertaining to the article.

To say that subscribers don't have consistent speeds from house to house or even neighbor to neighbor is a gross understatement. There is however a reason for this. Before any connection reaches a SHASTA or RADIUS server, the connection routes through either a DSLAM (Digital Subscriber Line Access Multiplexer) or a BSAM (Broadband Subscriber Access Multiplexer).These are the boxes located at the end of your street. They can generally handle anywhere from 8 - 400 customers and cost about $150,000 - $200,000 ea. The difference between the two is this; DSLAM's handle ADSL customers while BSAM's handle VDSL customers. Regardless of the type of service a subscriber may have, the connection from the box to their door is essentially the same. Every Subscriber is on what is called a loop. A loop is the section of cable to and from the phone jack to the BSAM or DSLAM. The farther a loop goes has a direct ratio to how fast and/or stable the connection is. The longest an ADSL line can be is about 3 miles. VDSL has a loop length maximum of about 0.8 miles. The main reason for the large difference is due to the massive data that travels down this line. The stability of the connection degrades very quickly over long distances. To sum this up, the longer your loop the slower/less stable the connection will be.

How to Hack it

Please keep in mind that this is information only. What you choose to do with it is solely your responsibility. I will not be held liable for any stupidity that arises from any misuse of this information.

It wouldn't be much of an article if I didn't at least share one hack, so here we go. As I mentioned in the beginning of the article, all DSL connections authenticate through a SHASTA. All service providers maintain a lot of them. This is a good thing. While all SHASTA's will communicate with the RADIUS server, they do not communicate with each other. For example, if you maintained more than one residence in town, there is a very good chance that there are 2 different SHASTA's servicing these locations. This means that the same uname and pword can be used in 2 locations as one SHASTA does not know that the other has already auth'd that username and password. This could allow you to maintain a server at one location and a regular internet connection at the other.

We pay enough for internet as it is these days. I feel you shouldn't have to maintain 2 accounts just because you maintain more than one residence or place of business.

Conclusion: Well, as my first article to Blacklisted 411, I hope you enjoyed the article or in the very least learned something new. If you have any questions or feedback, I would love to hear it. Please be aware that some of the topics discussed here have been generalized a little to improve the readability of the article (no one likes a manual).

Hack The System!

About The Author

Most people know me as TheInstallGuy, T.I.G., or that new admin guy @ blacklisted 411 forums. I have been involved in computers in many facets for about the last 20 years. My first computer was an Apple II C Plus. I programmed my first RPG game at the tender age of 13. It wasn't much, but it was better than Choplifter. Since then, I have maintained a steady interest in computers, mainly focusing on server deployment and network infrastructure. My hobby is all things wireless and radio. Currently, I reside up north in central Canada. Yes, it's cold 6 months of the year, no, we don't travel by dog sled, and yes, it's legal to reproduce copyrighted digital media for our own personal use.

Favorite Moment: Having a Hawaiian art gallery ask if extra packaging was needed on a painting being shipped. Apparently, they were concerned about it being damaged while it was transported by dog sled!? I wonder if they really thought I was going to hang it on the inside of my igloo???

Recently, I have decided to embark on the Blacklisted 411 Radio project. I will be working with Zack and Alex on this project and have a tentative date of mid September for the pilot episode. Please watch the forums for upcoming news and info on the show.

I will be sure to keep you all posted. Please feel free to email any ideas and comments at: theinstallguy [at] gmail [dot] com

Fixing Scratched CDs MacGyver-style

by Unic0der
unicoder@blacklisted411.net

A couple of weeks ago a friend of mine called me on Sunday evening and asked me for advice in a miserable situation: He had a scratched CD with extremely important data on it and he needed these data on the next day in the morning. Unfortunately the disk was in such a horrible condition that his CD drive did no longer accept the CD and the standard tricks like trying to read the CD with another drive or simply cleaning the CD with some cleaning agent did not help as well.

It was clear: What my friend really needed was a disk repair kit (one can buy in nearly every computer store), or even better, the help of a professional data rescue company. But he had neither the time nor the money for one of these options. So I told him: "Okay, sit down and relax, I'll find a way to fix your CD until tomorrow."

Let's do it MacGyver-style ...

My friend had nothing to loose, he needed these data now or never again. That meant for me it was time to try some of these crazy MacGyver-style CD repair tricks one can find all over the internet (Do you guys still remember the 80s TV series "MacGyver" where Richard Dean Anderson's alter ego could solve almost any problem by using science and his wits instead of violence? Good old times! ;-)). But let's continue with the story: Just like MacGyver I tried to find a solution to the problem by using only stuff everybody normally has at hands and by utilizing Google I found lots of tips and tricks on how to repair CDs with typical household equipment in a couple of minutes. While some of these tricks sounded pretty much stupid (like cooking the scratched CD in a bowl of water) some really seemed to make sense (like using car- or furniture polish). Since I had no idea which of these tricks really worked and due to the fact that there were controversial discussions on nearly all repair methods in lots of internet forums I decided to try them all to find out which one works the best for me.

So I took a couple of old CDs I didn't need anymore and scratched them until they were unreadable in both my hi-fi system and all my computer drives. Then I tried nearly all those crazy tricks from the internet, and guess what, I even tried the CD cooking trick; I mean hey, you'll never know, it may really work. ;-) But the results of my experiments were bad: Not only the CD cooking trick was (as expected) a total blank, but also tricks that seemed kind of logical to me did not resurrect any of my prepared Test-CDs, except one trick:

The toothpaste trick

Some of you may have heard about this trick before and thought it's a joke, but I can now confirm: No, it's not a joke! Polishing scratched CDs and DVDs with toothpaste is really the ultimate homebrew data rescue solution. (*Fig 1*)

But keep in mind that the whole procedure needs time (I needed over one hour to fix my Test-CD with the toothpaste trick) and that it's not guaranteed that the trick will work with every scratched CD. If the scratches are too deep or if the data layer on the upper side of the CD is damaged you will have no chance to resurrect the CD with this trick – no matter how long you polish. Also bear in mind that this is only a temporary solution to pull the data off the damaged disc. That means: Use the trick to resurrect the broken CD, immediately copy all data to your hard drive and burn them onto a new CD.

Here's how it works:

1. Apply the toothpaste to the data/rear side of your CD; Especially to the areas with lots of scratches. (*Fig 2*)
2. Before you start polishing the CD with a fine cloth or tissue wait at least 5 minutes.
3. Put some drops of water onto the CD and start polishing the CD (always rub from the inside of the CD to the outside, never rub in circles!). If the CD gets too dry while polishing add some more water.
4. After polishing a couple of minutes gently wash the CD with warm water (until all toothpaste is wiped off), dry it and test it in your hi-fi system or computer.
5. Repeat all steps until your CD drive can read the disk ...

That's it, it's really that simple. In this spirit let the toothpaste do the work, relax and hack the system. And

before I forget. Yes, the whole story with my friends CD had a happy ending as the toothpaste trick worked for him as well. J Peace!

Last but not least: If you have more time and money buy a disc repair kit or let professionals do the work for you. The toothpaste trick is only a solution for you if you have nothing to loose. The Blacklisted!411 magazine and I are not responsible for any data loss or damage caused by using the toothpaste trick.

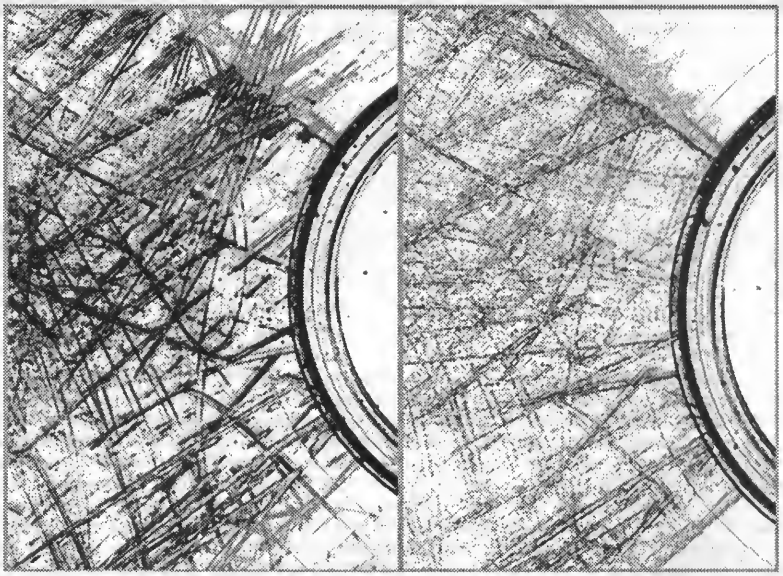


Fig 1: A scratched CD before (left) and after (right) the toothpaste trick. As you can see the heaviness of scratches is incredibly reduced on the polished disc. (Picture post-worked to improve the visibility of scratches)

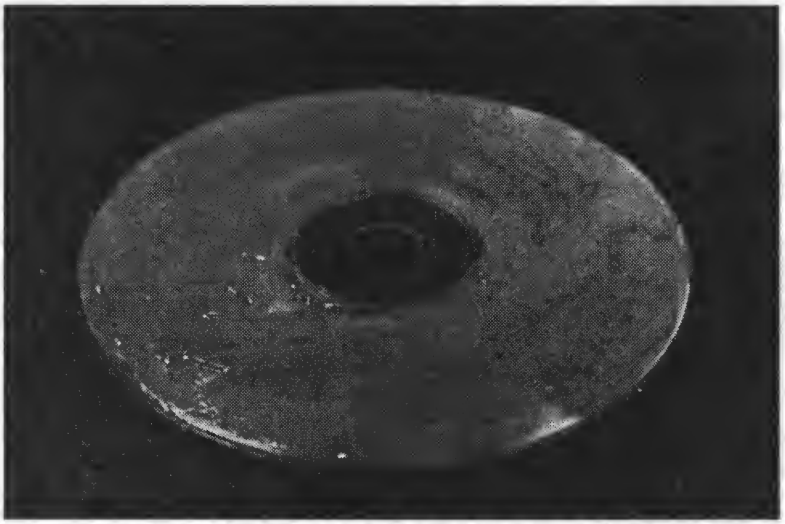


Fig 2: Put toothpaste onto the rear side of the CD and let it rest for at least 5 minutes.

THE RISE OF SKYNET?

By Rick Davis

Fans of the movie series Terminator will remember the global computer system, called Skynet, which was made by the military then ultimately grew self-aware and went to war with humanity. This is surely a far cry from today's technology however it does offer some insights and ideas for an advanced computer network. Also, while borrowing concepts from a movie genre it's hard to ignore The Matrix series which can also throw some inspiration for this project.

The purpose for this network was born from the need that myself and a group of friends had after our high-school and college days had passed and we scattered around the world to start our lives although we still wanted to do more than keep in basic contact through e-mail. Interest in various projects and many coming interests forced the need to share files and find a means for group communication that basic e-mail or phone could not provide. Also, our interest in distributed computing projects served by distributed.net sparked our interest in new projects and more productivity.

What we needed.

After a brief review of our needs we decided our Skynet needed to support these features.

- Central point for data storage and distribution
- Messaging system
- Varied levels of access
- Ability to easily add new systems
- Active security features

With these features in mind each system on the network would have specific access and roles.

Core – Central depository of data. Hosting of messaging system. Root network access.
Sentinel – Specific security related role. Access to core. Contribute to computing projects.
Node – Access point for each user to the core. Contribute to computing projects.
Drone – Minimal access, if any, to the core. Contribute to computing projects.

Network architecture.

The Core: The core itself was the most powerful computer on the network, built specifically with our goals in mind. It needed to have a lot of computing power to handle network operations as well as the storage capacity for all the users involved. Above all else it would need to be expandable and upgradeable for at least 3-5 years.

The most difficult part was the various permission levels of the data. Each user has a certain amount of storage space that only they have access to. Also, each user has a "public" area where they can place material securely and change the password when needed. There is also a general public area that all users could access. From there things got complicated. The bulk of the storage was broken down into three main sections, each needing increasing access. This was done because of the number of people involved. For example, the small group who started this project definitely wanted to share any material we placed on the core however the users we brought in to use their computing power did not get full access since only one or two of the "Super-users" would actually know these people. Then, somewhere in the middle would be those that contributed several systems or those that really had no interest in what we were doing. These users had varying access, usually custom defined.

Sentinel: Sentinels were our idea for active security. The initial design called for two and really there was no need for any more. One would continue to actively scan the network for virus and assorted malware threats. Scanning by the sentinels included the core as well as all nodes with "Super-User" access. The other sentinel would scan for intrusions. Mind you we were not worried about being targeted but rather random attacks and such we wanted to deal with quickly. The sentinel would log any activity and would have options for certain circumstances. For example, repeated attempts from a port scanner or anonymous access might see that entire subnet blocked.

Nodes: The nodes were initially the only other part of the network. These systems would be the primary systems that each of the original group used. In most cases this meant everyone's most powerful home

computer. These systems would be each users only link to the core and besides from participating in the functions the core provided the nodes would provide a major contribution to the computing projects.

Drone: A late addition to our plan which came from the idea to pull in as much computing power as we could. Users with more than one system could connect the others for computing support or any other needs that arose. Anyone that had an account would still only be able to connect from their primary system. Some group members brought in a drone system belonging to a friend or colleague for the rare need of a file transfer or if they were working on a project with any of us. In the meantime the drones would continue to provide added computing power.

Network hardware.

The only specific needs were for the core. It was designed for the most computing power with the available parts and funds. At the time this meant a dual-dual-core Opteron system with 4GB of RAM on each CPU. The RAM was expandable well beyond that and the CPU's were far from the best the motherboard could handle. The decision was made to get the core running and then as funding allowed upgrades and additions could be easily made. The massive case allowed for a floppy drive, a variety of optical drives and 10 additional empty bays. A 250GB hard disk formed "C" drive for the operating system and associated software. Then four-500GB hard disks formed the data storage area. The option was there for both the addition of extra drives as well as the replacement of existing drives when higher capacities when prices dropped.

All others systems spanned the full range of available hardware. Nearly all of the "Super-user" systems were at least a 2Ghz CPU although some of the drones were well under 1Ghz. Basically, any system we could access was brought in as a drone just for the processing power.

Network software.

Connections to the network were based on a VPN that the network operated from. All users had a login and password to access the network. Also, those that had a static IP had that address listed so that it was their only access to the network. Ideally, we would have liked everyone to have access limited to one IP address but that was not reasonable with standard ISPs.

It took a long time to decide on an operating system for the core but eventually the decision was to stay with a windows based system because of the variety of software available. Of course a server version was utilized. An intricate permissions system was spread throughout the drives and a commercial bulletin board program was set up.

For security standard commercial anti-virus and firewall software was used and a combination of freeware, commercial software and our own coding formed the security intrusion logging system.

Network permissions.

Probably the most complicated aspect of the system the various levels of access required a lot of thought. First, it was decided that absolute root access on the core could only be accessed in person while physically on the machine and this level of access would be required to affect anything on the super-user level accounts as well as network and software settings. . There were five "super-users" at the beginning and three were in close proximity to access the system if needed. Four of these five could create new accounts and permissions to effect all levels below themselves while the fifth was given this access only as a courtesy knowing they had no interest in dealing with the accounts although their knowledge in other areas made it important to have this access.

From there access was streamlined into four more areas. We were planning ahead incase we needed this much separation although at first we had only another 6 or 8 systems on the network. Access was organized into three levels of decreasing permissions (level 1, 2 and 3) along with another level which only kept in contact with the core and provided computing support. Accounts at level 1 had nearly all the access of a super-user expect the ability to create and alter accounts. Level 2 could only access limited areas of the core and most of time was not a permanent account. Level 3 was always a temporary account which we used for communication and file transfers to those that would likely not be visiting the network again.

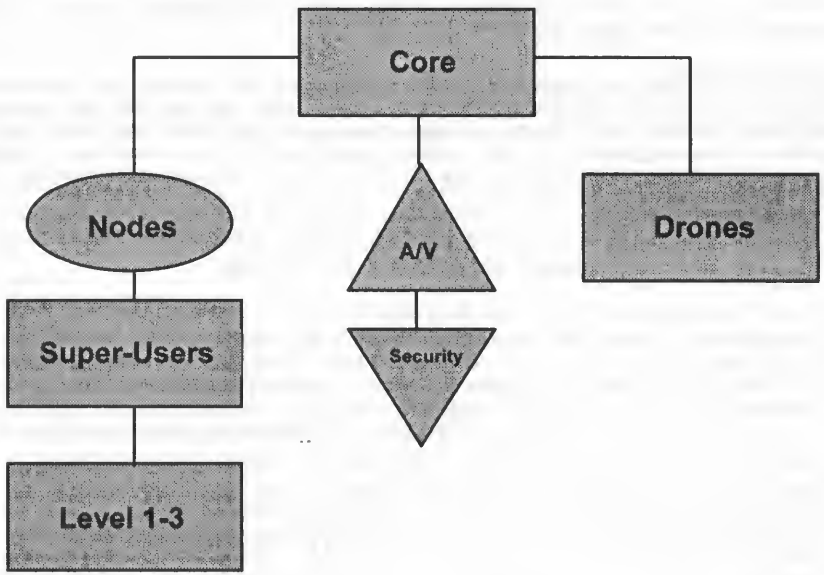
Aside from accessing the data on the core user access also limited what you could see on the bulletin board as well as information about the network in general.

Starting your own skynet.

Basically, the principles behind the network could be employed by anyone. Any computer can serve any purpose and instead of some costly software an FTP could be used for data transfer while a free bulletin board package could be run.

Depending on your resources, needs and number of users the general idea of the network can be easily adjusted for any needs. In fact, our design came out the way it did because of our limited money to invest in the project combined with our needs at the time.

Visual network representation.



Component / Access Level	Data / Forum Access	Admin Access	Other / Misc.
Core System	Storage of data and host for forum.	Physical access needed for super-user account changes. Physical access needed for many software and network changes.	Contribute CPU Power
Sentinel Systems	None.	Access only to areas relating to their tasks.	Contribute CPU Power
Super-Users	Private Directories. Shared Directories. Ability to create/delete some material and directories. Full forum access.	Set Permissions for all lower account levels.	Contribute CPU Power
Level 1	Access to a majority of storage. No personal directories. Forum access to all but super-user areas.	Some ability to create lower accounts.	Contribute CPU Power
Level 2	Selected access to data and forums.	Admin uses only given as needed.	Contribute CPU Power
Level 3	No forum access. Temporary access to specified directories.	None.	Contribute CPU Power Level 3 accounts are temporary.
Drones	None	None	Contribute CPU Power

A Blacklisted 411 Exclusive!

How to Secure Your Email

Written by Maxy

Each time you log into your email client or website, send or even just read emails, you leak a significant amount of information. Not only are your communications sent over networks as plaintext, and that mean's anyone with a packet sniffer who just happens to be on the same network as you—corporate espionage, anyone?—can read what you typed, but did you know that just by *viewing* an email you leak your Internet Protocol (IP) address to the sender?

In this article I will show you some ways to protect your IP; how to use secure, encrypted e-mail accounts, and how to help anonymize your email transmission/reception.

Secure Email Accounts

Chances are you use a free email account like Yahoo!, Hotmail, or, yes, even Gmail. The first option towards securing your email is to set up an alternative account on a secure server which encrypts the email transmissions for you, as well as masking your IP in some cases. The advantages of using secure email accounts is that you don't need to download any separate plugins like GPG or PGP and bother learning how to set them up, worry about incompatible Outlook plugins, and other such inconveniences. The disadvantages are, as we will soon see, limited storage space, and encryption limitations.

!Keep Your Secure Email Private!

A small caveat before we get into the gist of the article: although this may appear to be contrary to your common sense, consider that in some cases it may actually be advantageous to keep your secure email account private, releasing it only to close compatriots, and using a free 'unsecure' account (like Hotmail) for regular transactions—to keep those whom you don't want to know about the secure account in the dark! Think about it, the fewer people who know about your private, secure account, the fewer people can try to attack and compromise it.

With all this in mind, let's now look at some free secure email account providers available on the web.

MailVault
http://www.mailvault.com/

The Good Stuff: According to MailVault's About page, "MailVault's OpenPGP implementation is 4096-bit/1024-bit strong. MailVault supports 256-bit AES for SSL transmission security." The encryption keys are also stores in "distributed offshore servers" which are located in Malaysia. MailVault also allows you to import PGP keys into your keyring, which means that you can send encrypted emails to someone using their public key through MailVault, and the email will be encrypted against any eavesdroppers. The MailVault interface is also very intuitive and easy to use; fast-loading, and completely ad-free!

Looking at the *Received* paths in the headers of an email sent to a third-party account, you can see that MailVault also protects your IP:

Received: from mailvault.com (localhost [127.0.0.1]).

(I did not paste the entire header, as that would just waste space, though you can easily view full headers yourself in your favorite email program—in Gmail for instance, you can do so by clicking on 'More Options,' and then on the 'Show Original' link under the email Subject).

Whereas most popular non-encrypted email servers like Yahoo or Hotmail (though notable not Gmail) will leak your IP address.

Another interesting tidbit about MailVault comes from their FAQ (source: http://orlingrabbe.com/MailVaultfaq.htm), which states "the MailVault server will not permit connections from a **.gov** or **.mil** domain name. (If you are a slave of the nation-state, then humbly beseech your masters to provide you with private email.)."

And now the Bad Stuff: Email storage is limited to 4 Megabytes. That may be good for a few hundred small plain-text messages, but not very useful for sending longer encrypted text or any attachments. MailVault's 'off-shore server provider' also claims to provide DDOS protection (source: http://rayservers.com/new/ddos-protection), *however*, MailVault has just recently (at the time of this article's writing: Mid-August, 2006) recovered from a DDOS bounce attack (source: https://ssl.mailvault.com/DDOS_Explained.html). This resulted in a lot of legitimate incoming/ outgoing email not being delivered, and which therefore resulted in a lot of pissed off MailVault users! In fact, at the time of this writing (August 2006), when I attempted to send emails to my MailVault account from a Yahoo account as well as from a Gmail and Hotmail account, I received the following error from the mail daemon in all three cases:

```
This is an automatically generated Delivery Status Notification

Delivery to the following recipient failed permanently:

    XXXXXXXXX@mailvault.com

Technical details of permanent failure:
PERM_FAILURE: SMTP Error (state 9): 550 relay not permitted
```

This just goes to show that email servers are certainly not infallible, and you should take their promises with quite a big grain of salt. Though to be fair, keep in mind that *no* server is truly infallible against a sophisticated DDOS or similar attack, so don't think that MailVault is somehow inferior to the congested Hotmail, Yahoo, or even Gmail servers!

Also, while can send signed and encrypted emails to other users of MailVault, or to anyone who already has a PGP key from another service, you **cannot** send encrypted emails to someone without a PGP key or a MailVault account. And finally, MailVault does not seem to provide any sort of spam protection service.

Hushmail
http://www.hushmail.com/

The Good Stuff: Hushmail uses the Open PGP standard (RFC 2240 - http://www.faqs.org/rfcs/rfc2440.html) to provide 2,048 bit-strong keys, along with the AES encryption algorithm to encrypt the key. When selecting your passphrase, Hushmail lets you know the strength of the phrase (something the aforementioned MailVault doesn't do). Hushmail further provides a spam-filtering and virus-scanning service for free, as well as a Hush Messenger client for encrypted instant message (IM) conversations with your compatriots.

You can also export your Open PGP keys (both your private and keys). What this means is that if you are using Hushmail, you can export your public key and give it to a compatriot who is using MailVault, who will then be able to send you encrypted email from his MailVault account. Hushmail also allows the uploading of public keys, so you can send your MailVault compatriot encrypted email as well, using his public MailVault key. Hushmail further lets you setup a question/answer so as to be able to send encrypted email to someone even if they don't have their own PGP key. The recipient of the email will have to know the answer to a question you specify in order to be able to see your email.

Finally, Hushmail also strips out your IP from the e-mail headers:

```
Received: from hushmail.com (localhost.hushmail.com [127.0.0.1])
```

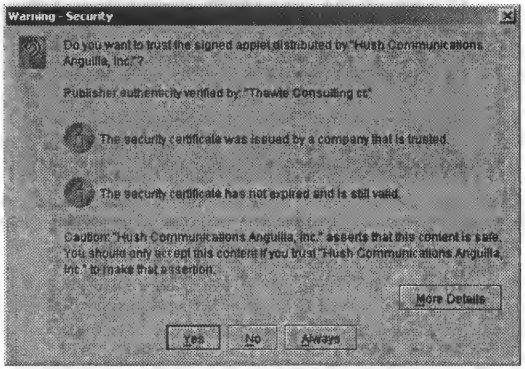


Figure 1 – Hushmail Security Dialogue. This screen appears when first installing the Hushmail encryption engine when you're signing into your Hushmail email account.

And now the Bad Stuff: Hushmail provides even less storage space than MailVault, clocking in at a mere 2 Megabytes. Free Hushmail email accounts will also be *deactivated* if not accessed at least once every three weeks (sucks if you're going on a retreat with no Internet access!), and you will then either have the option of purchasing a premium account, or having the email address deleted after six months (at which point an attacker can register that email account anew and then attempt to spoof your identity—this is a **very serious** issue, so if you decide to get a Hushmail account be sure to check it regularly to avoid losing it!).

With regard to security of the Hushmail servers, a little over a year ago in July 2005 Hushmail underwent a DNS attack (source: http://www.theregister.co.uk/2005/04/25/hushmail_dns_attack/) wherein users who typed in 'hushmail.com' into the URL field of their browser were sent to a different IP. This obviously presents the possibility for the phishing and keylogging of user passphrases. Hushmail blamed the attack on their domain name registrar, Network Solutions, and claimed that the data on the 'secure' Hushmail servers itself had not been compromised.

Lastly, the Hushmail encryption engine, which is Java-based and loads each time you login to the Hushmail website (or after each time you empty out your browser's cache—which you should do regularly) can take a while to load for 56K users, though to their credit there is an option to bypass the Java engine if you do not have install rights on the computer you are using.

CryptoMail
http://www.cryptomail.org/

The Good Stuff: CryptoMail appears to be another Java-based encrypted email option. The one innovative feature of CryptoMail is that it offers the option of sending your non-CryptoMail email account a notification each time you receive an encrypted email at your CryptoMail account. The sender's IP address, like with all of the other aforementioned secure email providers, is also protected (Received: from cryptomail.org (localhost [127.0.0.1]). I'm sorry, but that's about all the good stuff I could muster; on to the bad.

And now the Bad Stuff: The Java-based email interface is slow and clunky, which would be tolerable if you at least had the guarantee of strong encryption. Looking over the CryptoMail FAQs, Documentations, and so-called Technical Specifications, I couldn't find any mention of just what the hell kind of encryption algorithms CryptoMail uses. All the documentation in general is, in fact, very short and illusive, which leads me to believe the 'Snake Oil' corporation who owns CryptoMail (no, seriously, that's their real name) is deliberately withholding information from their end-users. When generating the keys, the interface said something about Open PGP, only to later state that CryptoMail is only "on its way to being RFC 2240 compliant", therefore apparently meaning that it's not even up to par with the Open PGP specifications?!

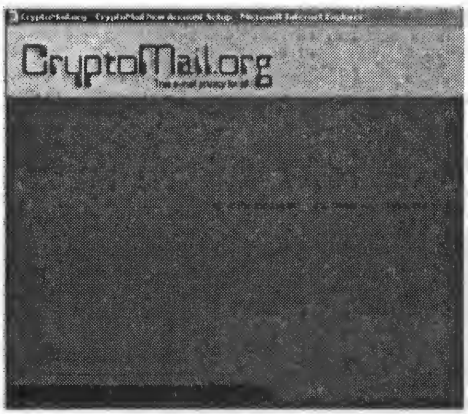


Figure 2 – CryptoMail Key Generation Screen. CryptoMail allows you to move your mouse around the screen to randomly generate a keypair, however, notice that they don't bother telling you what encryption algorithm and key-bit strength this generated keyset will use!

Furthermore, when looking at the raw 'encrypted' data generated only when sending email from one CryptoMail account to another, the 'encrypted' data was prefaced with "##################CryptoMail Version 0.1A##################". I find it just a little bit troubling that a service that claims to have been around since the year 2000 still uses an encryption engine that's version 0.1A.

And finally, as CryptoMail does not allow either the import or the export of public/private keys (and as I already mentioned, CryptoMail doesn't even tell you what algorithm these keys are based on, let alone the key-strength), you

can therefore only send encrypted emails to other CryptoMail users, not to mention that you don't even know the maximum storage capacity of your email box. Now, maybe some readers of Blacklisted are more intimately acquainted with CryptoMail, but until someone sets me straight, my advice is **do not use CryptoMail for securing your email.** We can not assume that their withholding of information is just due to simple negligence, and must therefore surmise that an ulterior motive is in place.

StealthMessage
http://www.stealthmessage.com/

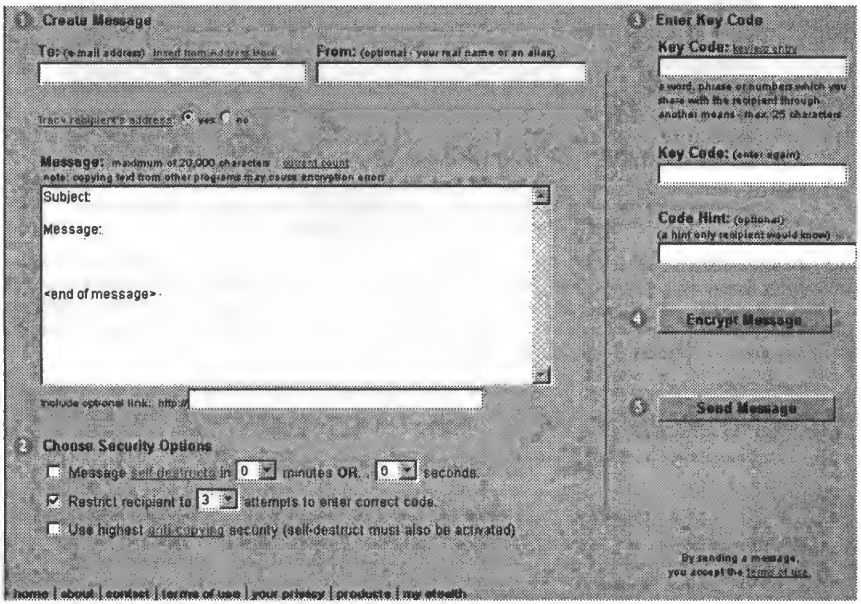


Figure 3 – StealthMail Email Creation Screen. StealthMail allows you to input your message, and set a variety of features such as self-destruction and anti-copying protection.

The Good Stuff: StealthMail provides a truly unique service which sets it apart from the three aforementioned secure email providers. StealthMessage provides 160-bit encryption with 128-bit SSL, but going further it offers several innovation features that are rarely seen in a free, secure email provider.

First of all, StealthMail provides the option of setting a 'self-destruct' timer for your emails. After the recipient opens your email, he has a limited amount of time to view it (which you set: maximum of 30 minutes, minimum of 1 second). You can also instantly self-destruct a message from your StealthMail account, which means that while the recipient will still be able to know that you indeed sent him a message, he will be unable to read it! This is a great feature if you change your mind about sending a particularly sensitive message. The self-destruct feature is also great for sending a short communiqué to a compatriot who is in a sensitive environment such as a workplace or public area where the chances of someone shoulder-surfing and reading the message are quite high, in which case you set the self-destruct timer to a mere one second, and—poof!—the message vanishes!

Secondly, StealthMail provides an anti-copying feature which prevents someone from copying the text of your message—a great feature if you want someone to read your message, but don't want them to retain a copy of it for evidence!

And thirdly, StealthMail lets you select the number of times you want the recipient to be able to re-enter the passphrase to be able to read the email, which will prevent an attacker from brute-forcing or even just randomly guessing your keyphrase.

Finally, as is to be expected, the StealthMail messages arrive at the recipient's inbox from a randomly generated StealthMessage.com account, with the Received field saying: from EWHSERVER122 (unknown [10.10.13.1]), thus masking *your* IP. The body of the email then says "A private message has been posted for you from whoever@whatever.com" and directs the recipient to go to a secure StealthMessage website and enter his passphrase so as to be able to view the email message.

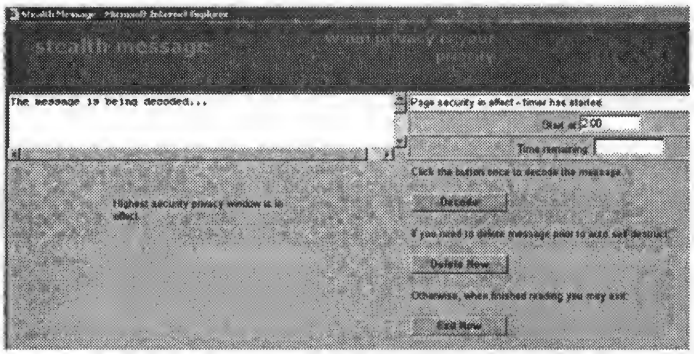


Figure 4 – StealthMail Message Receipt Screen. After the email recipient enters his passphrase that you (as the sender) agreed upon with him, he'll be presented with this Message Receipt screen. As soon as he clicks 'Decode' the timer will start ticking down until the message self-destructs. Neat!

And now the Bad Stuff: Unfortunately, most of StealthMail good points also have slightly negative counterparts. The anti-copying feature can easily be defeated by taking a screenshot (even if StealthMail designed their scripts to disable the Print Screen keyboard key, you could still use a third-party screen grabber program, there's tons of them around). Likewise, the self-destruct timer you set may not be enough for a recipient with a slow computer or who is a slow reader and doesn't finish reading the message within the allotted time.

However, the biggest inconvenience of StealthMail is its requirement that the recipient enter a special passphrase—which you two will have to have previously greed upon in advance—in order to read the message. It is imperative that you two agree on the passphrase in a secure environment—not a plaintext instant message conversation or in a place which may be bugged or otherwise monitored/surveilled!

Conclusion

So out of these four aforementioned secure email services, which one would I recommend? Well, assuming that MailVault successfully recovers from the DDOS bounce attacks and you're able to both send *and* receive emails from/

to the account, they would definitely be my first choice based on security and ease of use. Following MailVault, I would pick Hushmail as my second choice, due to its somewhat clunky interface, which is nonetheless compensated for by its wealth of available features. StealthMessage would come in a close third place, due to the fact that you can't export or import encryption keys, yet I very much like its innovative self-destruct feature. Finally, the mysterious CryptoMail would come in at a far fourth place, as I guess it's still better than using completely unencrypted email like Hotmail, though I'm not sure just how much better it actually is ;)!

If you don't like any of these secure email providers, you can always run your own Simple Mail Transfer Protocol (SMTP) server (assuming that your Internet Service Provider (ISP) allows you to do so!). One such server is called 'Email Privacy' (source: http://www.download3000.com/download_4469.html) and turns your own computer into a secure SMTP server for sending emails directly to your compatriots using any other third-party email program such as Microsoft Outlook, bypassing any mainstream email servers, and therefore lessening the chance that your email is intercepted. Though please note that this doesn't guarantee security! As such, I would highly recommend encrypting emails, not just sending them from your own SMTP server.

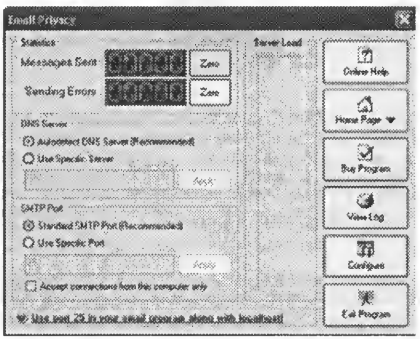


Figure 5 – Email Privacy Main Screen. A screenshot of the shareware version of the email privacy SMTP server program. As the full version costs almost $50, I, unfortunately, could not experiment with the full version and more fully report on its functionality.

Finally, remember that these are just four secure email options out of the hundreds that are out there. My reviews are simply meant to get you to start thinking cogently about securing your emails, and should be taken as a guide to exploration on your own! When you google "secure email" or "free encrypted email" and see lots of different corporations offering their services, **be very skeptical** and be sure to evaluate each email provider **at least** on these points:

- Level of encryption
- Protection of sender's IP address
- Mail storage space
- Allowance of the importation/exportation of encryption keys
- Customer reviews of the service
- Any past attacks like DDOS or DNS hijacking against the mail-server
- Anything else you feel is important!

I wish you luck in your search for and use of secure email services, and remember the warning of keeping your secure email private given at the beginning of this article—so as to keep it from falling into the wrong hands!

Notice of Non-Affiliation and Disclaimer

I am neither affiliated with nor in any way compensated by any of the companies and organizations mentioned in this article. The opinions stated herein are just that: opinions, which are my own and do not necessarily represent the views of anyone but myself. They are not necessarily the views of BlackListed 411 or of any of the mentioned companies. This article is presented for information purposes only, and I will not be held responsible for any misuse of the information contained herein, or any data loss resulting from the use of said information.

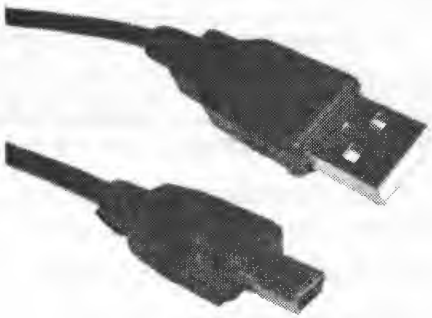
MODDING THE MOTOROLA RAZR V3

By M@

This article is one of many that I will write dedicated to giving others the correct information about modding the Razr V3. I have owned my V3 for a little over a year now and have had endless amounts of fun with modifying it. I hope this article, and the others to come, sheds some light on what is possible for the V3. That being said, I will accept no responsibility for anything that goes wrong with your phone. I'm giving you all of this information on a trial and error basis. (I've done it myself and this has worked for me, and will work for you if done correctly. Don't do something to your phone if you're not sure what your doing. Ask first!)

Introduction

First off, V3 modding is usually done with something called a data cable. This cable will allow you to connect your phone to a computer. It looks like this:



You can buy these cables from your Service Provider or from the Internet, however, you may have noticed that there really isn't anything special about this cable. It's just a standard USB cable with a mini 5-pin USB head on the other end. In fact, if you have a digital camera, check the cable that came with it. Chances are that cable will work fine for your V3. If you don't have a camera, head on over to an electronic store and shop around for a cable that would work.

There are many programs out there, some of which will be covered later, that allow you to use Bluetooth technology instead of using a data cable. However, I don't know a lot about Bluetooth and I know that a data cable would be the better way to go because most programs recognize a cable rather then Bluetooth.

Terminology

I don't know about all of you, but I hated this in English class, but I will try to make it as painless as possible. There are a few terms that many of you may already know, or you're hearing them for the first time. Either way it's important to have an idea of what it all means BEFORE you start modding.

Flash – The Flash of a V3 can most easily be described as the Operating System of the phone. It is the most common thing you will modify on your V3. When you flash your phone, you will not lose any of your media on your phone.

Flex – These are the files that contain the Service Provider's "branding" on the phone. (start up animation and sound, shut down animation and sound, and other labels) They also include all the programming needed in order to connect you to their Internet service and text messaging on their network.

Bootloader – This operates like the BIOS on a PC. It's software telling the phone what is what and where it can find everything it needs to function. It can be upgraded and downgraded. Most modders (like me) downgrade it. It was the first thing I did on my V3 because some programs may not work on later versions of bootloaders.

Seem – Seems control every single aspect of how the phone operates. "SEEMS are storage containers for Phone Settings information...Each setting is stored as a single bit, which can have a value of 1 or 0. Often, the value of a bit is represented by a check box, Checked = 1, Unchecked = 0." –Manalive

Unlocking – There's some discrepancy as to what an "unlocked" Razr is so this should explain it. An unlocked Razr means that it may be used on other Service Provider's networks freely. Service Provider's lock the phone making it difficult for users to switch networks and keep the same phone. More on this later.

GSM - Global Systems for Mobile Communications. GSM based phones, (like my Razr) have a sim card in it. (The little chip near the battery that holds all of the Service Provider's information and can be used to save your phonebook, etc.) GSM is nothing more than a network type. It allows easy switching between Service Providers.
Ex. T-Mobile, Cingular, Rogers Wireless, Fido, etc.

CDMA – CDMA stands for Code-Division Multiple Access. Arguably not as good as the GSM based phones, due to the fact that it's old technology and does not use sim cards. Also, CDMA based phones use software called BREW. (Binary Runtime Environment for Wireless) BREW is the hardest software to modify on these types of phones. In fact, most of the programs out there only work for GSM based phones, so that's a major downfall.
Ex. Verizon, Bell, Alltel, etc.

Get Started
Now, assuming that you have your data cable and ready to begin, you'll need to get your hands on a folder called P2K Drivers. These drivers will allow your computer to recognize your phone's new hardware when you connect it to your computer. You can get them here:

http://themotoguide.com/index.php?PID=1&PGID=430&PHPSESSID=eea0b329229df215c75e52227d7ac71b.

Also, you'll need a copy of RSD Lite. This program will allow you to flash/flex your phone. (We will discuss that later) For now, you'll need to download it, from the url above also, and don't install it just yet.

When you connect your data cable to the computer, then your phone to the cable, your computer will recognize new hardware on your computer. When you open the new hardware wizard, select the option to "Install from a list or specific location (Advanced)" At the next window, uncheck the "Search removable media..." box and check the "Include this location in the search". From the drop down menu, navigate your way to the P2K drivers folder, (uncompressed of course) then click next. It should install the Motorola USB Modem for you. When completed, click finish.

Now, you can install RSD Lite. Follow the on screen instructions to install it. When that's done, open up RSD Lite. With your phone still connected, the new hardware wizard should pop-up again. Follow the same instructions as before, selecting the P2K Drivers folder. When that's completed, the wizard should show up again. This time, leave the "Install the Software automatically" selected, and let it do its thing. There should be only one more hardware installation. Just do the same thing for the rest of them. When it's all done you can close RSD Lite for now.

Downgrading the Bootloader
The main reason why you would want to downgrade the bootloader is due to RSA protections on the phone, basically policing you from doing what you want. (Which for some, can be a good thing)

Before going any farther, you'll need to know the current bootloader on your V3. To find this out, turn your phone off and then press and hold the * and # buttons while hitting the power button to turn it on. A black screen should appear showing you your bootloader version, (Mine was 08.26) and SW Version. (The flash of the phone) If you see that you have version 08.26, you'll need to use a downgrader program. A good one can be found here: http://rapidshare.de/files/13848110/scotty2_8.26_downgrader_v2.zip.html. It's called Scotty2 Downgrader. Only version 08.26 users should use this program.

If you see that your version is 08.23, you should not use this program. In stead, you'll have to flash the R374_V3BL_07.D0 bootloader on to your phone. I will cover how to flash your phone later in this article. You can find this flash bootloader at: http://rapidshare.de/files/13842811/R374_V3BL_07.D0.zip.html.

Eventually you will end up with 07.D0. This is the best bootloader to use and you'll never need to change it again.

Caution: Make sure your battery is fully charged. Make sure you have a stable connection to your computer. Don't run any other programs when using the downgrader. **Proceed at your own risk.**

All you need to do is connect your phone to the computer and run the downgrader. It's a completely automatic process and should take about 5-6 minutes.

For the rest of you, who have 08.23 and lower, all you'll have to do is re-flash that bootloader to your phone. For this you'll need RSD Lite. Then follow the instructions for flashing the phone further down.

Backup Your Phone
This should be, clearly, the most important step you do before going any further. I will show you how to backup your calendar and phonebook first. You can do this with a program called Motorola Mobile Phone Tools or DataPilots Universal Essentials. I will explain how to use MPT, because that is the one I am most familiar with, though I'm sure DataPilots isn't that hard to use.

You can get MPT from Motorola, your Service Provider, or of course the Internet. I would suggest finding a cheaper version of it on the Internet somewhere. Just search around and you'll find it no problem.

Once installed, and your phone is setup, a little picture of your phone should show up on your computer screen. When you see this, click on the menu button on the keypad, then click Organizer, then Mobile Phone, and finally Backup/Restore. Then you should be able to follow the on screen instructions for backing up your info. Make sure you know where your backing up your files.

Next comes backing up your system files. Get a copy of Flash Backup from here: http://www.mark-world.tv/motorola/page1.html. After launching it, select Backups at the top. Select Full Backup under Backup Mode. Under Phone Memory Size, select 32 MB. Check the box saying Disable Backup Compression...Now go to the area that says Select Loader (Only For Advanced Users) and choose Select Another. After a pop-up shows, navigate to the installation directory for Flash Backup, and go to the folder named RamDld Pack. Select the 32 MB (08A0).ldr file and click open. Now just click create. When it's done, you'll be left with a single file. Success!

There are two other backups you can do also. (A bootloader backup and a PDS backup.) For this, do the same as before, but this time just choose the correct backup type from the Backup Mode drop down box.

Flashing the Phone

For flashing your phone, you'll need RSD Lite and you'll need a re-flash file. Go to http://www.planetmotox.net and find a new flash file for your carrier. (ex. Cingular)

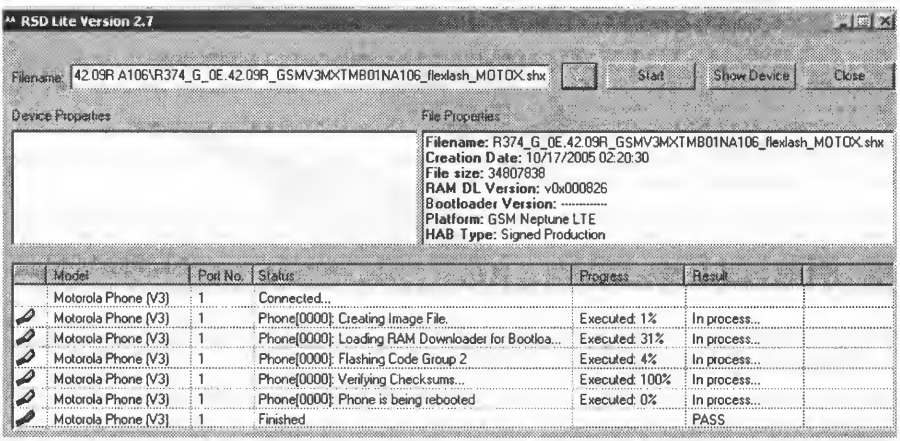
Launch RSD Lite and plug in your phone into the computer. It should detect your phone right away. If not, turn your phone off and turn it back on in flash mode (* and # upon startup.) After it detects your phone, click the ... button. Navigate to your new flash file that you got, then once selected, click Start. Your V3 should display a black screen with SW Upgrade in Progress on it. When it's done, click close and your done.

Flashing your phone should not delete any personal files on your phone, however, if you have something on your phone that you don't want to lose, highly suggested that you back it up before you start.

Flexing the Phone

As you should know by now, the flex of the V3 are the files that contain your Service Provider's branding on the phone, and also include the programming needed to connect to their network. You don't really need to flex your phone unless your goal is to unbrand it or because you purchased a used phone with outdated software on it. I never flexed my phone, there was no need to, but I will show you how to do it.

First you'll need a new flex file. Head to http://www.planetmotox.net and find yourself the newest flex file. We will use RSD Lite for this process as well. Launch RSD Lite and plug your phone into your computer. Once RSD recognizes your phone, click the "..." button and locate your new flex file. Once you've found it, click the start button. Once it's done just close RSD Lite.



Screenshot courtesy of http://www.mark-world.tv/motorola/page1.html.

Again, I really found no need to flex the phone so don't be in a big hurry to do it yourself. The only reason, I can think of, why you'd want to flex your phone is if you have one Service Provider's branding on the phone but you're using services from a different provider. (Ex. You bought a used phone.) Also, when you flex your phone, it will delete all of your personal files from the phone. (Photos, ringtones, etc.)

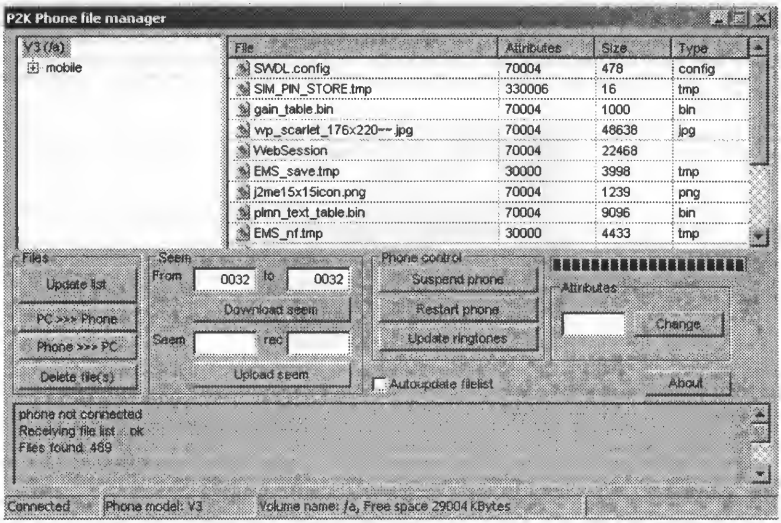
Seem Editing

I have just recently discovered seem editing, and the wonders it holds. Seems basically control the flex of the phone by activating and deactivating features on the phone.

I will cover two seem edits. (One from the 0032_0001 seem, and one from the gain_table.bin seem. All of this will become clear in a few minutes.) You will need to use P2K Phone File Manager (P2K Man) to download and upload the seems from and to your phone, and you'll need XVI32 to edit the downloaded seems. You can get both of these from here: http://www.mark-world.tv/motorola/page1.html.

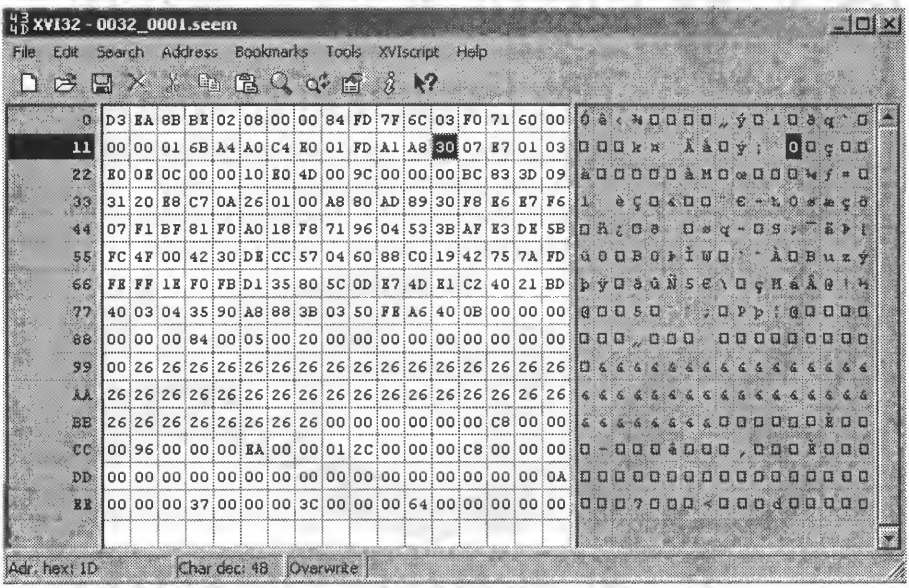
Now let's begin with the gain_table.bin seem. For this seem edit I will show you how to turn up the earpiece volume for a phone call.

Launch P2K Man and connect your phone. It should recognize it right away. When it does, hit the "update list" button. Look in the /a directory (on the left) and on the right look for a file called gain_table.bin. When you find it, select it and hit the "Phone>>>PC" button. This will download the file to your computer, of course. After the file downloads, you can close P2K Man for now.



Screenshot courtesy of http://www.mark-world.tv/motorola/page1.html

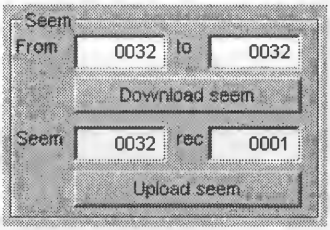
Launch XVI32. Before you open your file, you need to make sure your viewing hex instead of decimal. To make sure this is the case, just click on options, then data inspector.After that's done, click the open button and select your gain_table.bin file. When it opens you should be left with a table full of numbers and letters. Make sure the "big-endian (Motorola)" is checked. Leave the options. Now your ready to open your file, so go to Open and find your gain_table.bin file. When it opens you should see a table full of letters and numbers.



Screenshot courtesy of http://www.mark-world.tv/motorola/page1.html

These are the things you change when you do seem editing. Look at the bottom of the window when you select one of these numbers. It gives you a hex address. (The screenshot above shows the address 1D) Look for a hex address "D". (Or 0D) it should be right at the top, and fourth one in from the right. This is the offset that controls how loud the earpiece is for a phone call. (The default setting is 1 of course.) I changed mine to 04 and it works perfect. I can even hear the person when I'm outside with lots of background noise, and it's not so high that I need to worry about blowing the speaker, so I would recommend 04. To change the value, just select the offset, (01) and type in 04, and it should change for your. Next, save this new gain_table.bin file.

Then quit XVI32, and re-open P2K Man. When the phone is recognized, hit "update list" again. Make sure you don't have a gain_table.bin file still in the /a directory. (Delete it if it's there.) Now, making sure that the /a directory is selected, click the "PC>>>Phone" button, and locate your gain_table.bin file and upload it. When it's done, hit the restart phone button and let your phone restart. Vuala! Now you should be able to hear the person you're talking to next time you call someone, or someone else calls you.



The next seem edit I will show you will allow you to keep a speaker phone call active even with the phone flipped shut. For this, you'll need to open up P2K Man again. Once you've updated the list of all the files on your phone, go to the "Seem" area and enter "0032" in the "From" box and "0001" in the "to" box. Click download seem. Save the seem file to somewhere you can find later. (Obviously) Next, open up XVI32 and load your downloaded seem file. Click on offset 8A to select it. Click on Tools and select Bit manipulation. In the "Status of Bits" area, uncheck bit 2. When this bit is unchecked, you will be able to flip the phone shut while on speaker phone and still be connected to your call. If it is checked, your phone will hang up the call when flipped shut. Now save this newly edited seem file, and upload it to back to the phone using P2K Man. To do this, enter "0032" into the "Seem" box and "0001" in the "rec" box. Hit upload seem. Locate the new seem file and hit open. Tah Dah!

That's the basics of seem editing. There is a great seem map on all the different seem edits you can do at :

http://www.mark-world.tv/motorola/doc/seems.doc. It is updated by http://xlr8.us/hofo.

cl.gif Changing
Ever wanted to change that outer LCD image on your V3? Typically it has the name of your Service Provider on it and nothing else. Well never fear, something can be done about this. All you need to do is find a .gif image of your choice, (some can be found here: http://www.motox.info/showthread.php?t=435.) and make sure it has the proper proportions. (96x80 pixels) Using P2K Man, all you need to do is navigate to the /a/mobile/skins folder and find the file called cl.gif and delete it. Now all you do is hit PC>>>Phone and locate your new cl.gif image. (Be sure to name your new image cl.gif. Also the picture must be a .gif format or it won't work) After that's done, restart the phone and check it out. Cool, huh.

Custom DRM Icon Sets
Installing your own icon sets are surprisingly easy. All you need is a .shx icon file (filled with all the new icons, duh.) and just follow the instructions for flashing your phone. (Using RSD Lite.) You can find some cool icon sets here: http://www.mark-world.tv/motorola/page10.html.

Custom Start-up and Shutdown Animations
Putting on your own start-up and shutdown animations is always a cool idea to give your phone some style. All you need to do is connect your phone up to the computer and load P2K Tools. (Found here: http://www.mark-world.tv/motorola/page1.html) Once you have that loaded up all you need to do is hit "tools" at the top and "custom animation." Now from here it's pretty straight forward. All you have to do now is check the box on the left of the start-up and shutdown animations and locate where your .gif files are on your computer. Then restart your phone and your done. (you can follow the same steps for putting on your own start-up and shutdown sounds)

Cleaning Inside the LCD
This used to really bug me with my phone. No more than a week after I got it, there was dust accumulating under the screen. I found myself rubbing the screen so much I was slowly going insane. So I looked into cleaning it out for myself, rather than having to send it all the way to Motorola just for some guy to wipe it out. Here's how I did it. (Official manual, with pictures here: http://www.mark-world.tv/motorola/pdf/Getting_the_dust_out.pdf.)

All you need is some sharp end tweezers and a new LCD cover. I found one at http://www.cellphoneshop.net. Use the tweezers to pry under the LCD cover. Once you have it, just pull up and it should come right off. Now take your new LCD cover, remove the plastic from it, and starting at the bottom, line up the new LCD cover with the inset. Be sure to apply even pressure across the edges to make sure it sticks in place. Vuala!

Conclusion
Well that does it for my Motorola Razr V3 modding guide. I hope the pictures I added, courtesy of http://www.mark-world.tv/motorola/page1.html, has helped at least a little bit. By now you should have more than enough knowledge to do your own mods without much help. Again, be sure to ask about anything your concerned about before you start modding. (It's your phone, not mine. The info. I share with you has worked for me and should also work for you, but I will not accept responsibility if you brick your phone. You have been warned.) I will be sure to work on a third and final edition to this series, mainly consisting of little mods you can do to your phone easily. Well that does it for me. Talk to you soon.

About the Author

My name is Matt (M@) and I live in Canada, eh! I'm in my senior year of high school. I am athletic, outgoing, and have been interested in technology ever since I got my first gameboy color, way back in the day. I mainly stick to cell phones, computers, MP3 players and gaming consoles. My favourite food is Fettuccini Alfredo, and I love Mountain Dew. My email address is chalupaman_99@hotmail.com.

I-HACKED STAFF HACKS 2006 DEFCON HACKER CONVENTION

By: Hevnsnt

What happens when you place 6,000 of the worlds best hackers in one hotel? Stuff gets hacked, normally the hotel's stuff. This year, Surbo and I wanted to change that -- and this is the story of how we did it. We made the sacrifice to put our lives on hold and go to Las Vegas (yeah it was rough) to mingle with the worlds best hackers. As we got there and checked in we were given the lowlyest of badges, the "General Population" badges -- referred to as the "Human Class". Don't get me wrong, Joe Grand (of GrandIdeaStudios.com) did a great job on the badges, but did I-hacked staff deserve the plain "Human" class badges? We certainly didn't think so, later we will discuss how Joe's design ultimately led to the compromising of Defcon.

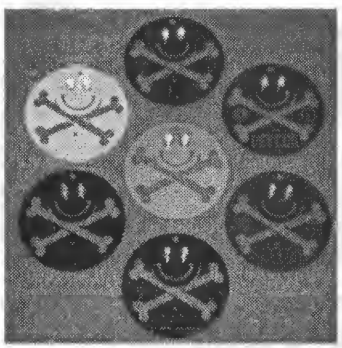
After we had received our badges, we made a short trip back up to the room to do a little modding to the badges. After 10 minutes of pulling apart official I-Hacked Throwies and soldering we had modded our badges to stand out from the crowd. Happy but not satisfied, we strutted our stuff among the crowd as quite possibly the first to "mod" their badges. As we explored the convention center we found our way (passed some velvet rope) to a hallway that was protected by a guard. Without any discussion between us, we both knew that we wanted passed the guard. As nonchalantly as possible we struck up a conversation between the two of us and tried to walk passed the guard as though we were meant to be there. Politely yet firmly the guard told us: "Red Badges Only" and told us to leave.

As I had been to a 'Con before, I knew that "Red Badges" meant one thing, and one thing only. Goons. The holy grail fear of any Defcon goer, the goons are the elite of the defcon staff. We wondered what wonderful things they had down that hallway, surely they had gigabit connections, imported beer filled swimming pools, and rainbows made of skittles. We had to get back there to find out. We decided it was time to figure out exactly what the other color badges looked like. Surbo put on his social engineering hat and asked the registration desk: "What are the red badges for?" The goon who at the time was wearing a red badge replied smugly "You have obviously never been to a con before." While surbo's job was to pull information from the registration guy, my job was to get a close inspection of the badge. At this stage we were still gathering information, an important step in any hack. Gather as much information on your target as possible, then take your time and have a beer.

Speaking of beer it was time to hit the strip, we packed up and walked down to the main strip. We toured a lot of the different bars around, but because it was a thursday night nothing was really happening. This was not my first trip to vegas, but I still wanted to see all the street shows again. As surbo and I walked up and down the strip we stopped to see the Treasure Island show (pirates kick ass), some guy who was doing incredible artwork with spray paint, and some really crazy bands performing in each one of the casinos we ducked into to grab a beer along the way. Anyway, enough about vegas, lets get on to the hack already.

The next day (friday) was the beginning of Defcon and the crowd was among us. The amount of people that showed up for this years defcon was absolutely staggering. I don't know the official number but I do know that it was well over 6,000.

We had had a night to discuss what we thought about the badge. We had already scanned our badges with our favorite RFID Scanner (APSX RW-310) and could not find any trace of signal. Our program manual stated that Joe Grand would be giving a talk about the badges the next morning -- maybe he would talk about the differences of ours vs. the other color badges.



All the different colors available

During Joe's talk he started discussing the process of creating the badges. He mentioned that the cost per badge had to stay below $5, so it became apparent that there probably wasn't any embedded RFID in the other colored badges. Then he finally talked on how he created the different colors, he simply used a colored solder mask to create the different badges.

BINGO. Thanks Joe!

The only difference between my badge (white) and a Goon badge is the Red color. On the way out of the speech, I looked at surbo and I could tell he was thinking the same thing I was... Lets go visit the spray paint artist on the street.

Later that afternoon, we left our hotel and defcon festivities behind to go see the guy who would change our defcon experience for exchange of nothing more than a I-Hacked throwie that he could place on his lamp. I showed him a picture of the red badge that we would like to emulate, and he mixed and matched his colors to get it perfect.

Um, I would like it Red Please.

Simply put, it came out perfect. As far as anyone was concerned we were now official Defcon goons. We only had him paint the front of the badge red (and left the back white) so that we could later prove to the security staff how weak their security measures where.. This later turned out to be a bad decision. (but I wont get into that just yet) =p

Later on that night at the private parties (as goons, we didn't have any trouble just walking in now) when anyone asked if we were goons we would just nod our head yes and switch topics. We didn't want to blow our cover just yet. We were in the penthouse suite, partying with the guys who put on defcon -- we introduced ourselves to as many people as we could to get a few names to drop if needed.

Saturday: Completely hung over, my only goal for that entire day was to see Dan Kaminsky's talk on net neutrality. As we finally made our way down to see his talk, we found the room to be completely full. No one else was being let in. Surbo had noticed the day before that the Goon HQ was a skybox overlooking the particular conference room where Dan was giving his talk. Being as though I really wanted to see this presentation, we made the call... It was time to try out our goon badges.

As we made our way down the hallway, we passed the guard with out any incident. In fact she even stopped a few other people who tried to surf in with us. (Sorry guys, apparently you need a Red Badge to get past her =) We were now past the guard, finally in "Goon-Land". We tried door 1, Locked. We tried Door 2, Locked... Arrgh Out of desperation, Surbo knocked on door number two. A few seconds one of the largest goons I have ever seen opened the door and asked what we wanted. Surbo said "XXXXXX told us to come up here to watch Dan, to give up some seats. (XXXXX's name has been removed to protect him, lets just say it was one of the names we snarfed from the party the night before)

Without hesitation, he opened the door and took us out to the balcony. Now unless you were there you can't imagine the tension. We are completely surrounded by goons, in their room, with fake goon badges. I snapped a few pictures as proof from there as discreetly as possible, but they turned out horrible. None of the other goons were taking pictures so I figured I should lay low with that.

During Dan's talk, a goon walked out on the balcony with a huge juicy steak. We hadn't eaten yet, and damn that thing looked good. As soon as the talk was over I asked the goon "Where did you get the steak?" and he looked at me a little weird and said "The Refrigerator" and then walked me into the kitchen and showed me exactly where.. =)

Fast forward to later that night. The badges opened up more than physical doors. We were now invited to the best party of the 'con (Ninja Party absolutely rocks) where I had a few too many drinks. After bouncing between Ninja, the White Ball, and the pirate party (all of which I continued to drink) surbo decided to leave me to my own fruition. (Mistake #1)

Well my liquid courage had set in, so I figured that I would go tell the goon squad exactly what I felt about their physical security and identification methods. I stumbled right passed the security guard, and at no time did I question what I was about to do. (Mistake #2)

Ready for mistake #3? I threw open the door to Goon HQ, and was presented with a room full of goons (Seriously it was somewhere around 4am, and there was probably 15 goons in there) and sitting in a chair right in front of me was the head of security, Priest. (Which btw if you have never seen him, is a big dude) Undaunted, I began my speech about how I was able to bypass all of their security methods using a can of spray paint.

Lets just say, that this probably wasn't one of my shining moments. Sure, I had proven that I could bust their security. I had proven that when it really comes down to it, I have a sack of fortitude, and I had proven that after all that beer I really need a second opinion on things. =)

Priest was incredibly cool, and although he confiscated my badge he told me to get a hold of him in the morning.

Sunday morning I found Priest; and after a stern warning about next year he told me. "Good job, you hacked defcon. You made it past our security. For that, I am going to get you another badge, another WHITE badge" I of course appreciated this, but I asked for my original badge back, I mean it meant so much to me. He told me that it had already been destroyed, but I like to think that he has it hanging up as a memento of Defcon14.

Fare well Badge, thanks for all the fun.

Sure this wasnt the most "Elite" of hacks out there, but it really goes to show how something as simple as spray paint can be used to circumvent some of the most sophisticated security forces. I hope you liked the story, and I can't wait for DC15.

Defcon Physical Security Hole

Written by: Matrix

My name is Matrix. No, that's not my real name, but people know me by this name. I'm a regular Defcon attendee. I'd like to think that most of the other regular Defcon goers know me very well. For those who do not know me, my specific daytime job is supervising physical security at a nameless technology center. Enough about me. Let's get back to the subject of this article: Defcon. I have been attending Defcon for well over a decade. One could reasonably argue that I'm one of the original attendees. I mention this, why? During my many trips to Defcon, I've witnessed just about every conceivable situation over the last 12 events. I was sure that I've seen everything possibly imaginable.

I attend Defcon for a couple of reasons. Well, three if you really care to know. I like to party. I need not explain. I enjoy technology. Again, no explanation necessary. I enjoy the company. I like to surround myself with the kind of forward thinking people who attend Defcon for personal satisfaction and to help expand my job skills. My job depends on understanding how people think. Who better to learn from than the best of the best. Oh, I also enjoy the various competitions and speaker presentations. I particularly enjoy the scavenger Hunt. Shouts to Vegas 2.0!

This year, while I was somewhat apprehensive of the new venue, I was happy to stand in line and wait it out. What appeared to be yet another "typical" event, I quickly changed my tune. I was immediately aware of a possible security flaw when I got my first glimpse of one of the Goon badges. Those beautiful RED badges! The possibilities began to spawn while I stood there. I tuned out my buddies and began to consider the options.

Here was the key problem with Defcon security this year. The *ONLY* difference between the goon badges and the human (uh, that's us regular folks for those who don't know the lingo) was only a matter of color. The color of the solder mask, that is. Goon badges were RED and human badges were WHITE. It was conceivable that simply painting the white badges with red paint would grant immediate access to goon territory. I later found out that I was correct. Very correct!

You see, in the security field, difficult to duplicate VSE's (or visual security elements) are vital to a strong physical security barrier. Without this, anyone with the know-how can easily bypass this most basic first defense and render the entire security solution useless. The most basic VSE is an "overt" VSE which means that the security element (in this case, the color of the badge) is easily visible to the human eye. Overt VSE's are designed to make ID authentication easy to verify. Next, you have Covert VSE's which are, you guessed it, not visible to the human eye. An example of this would be a hologram or "invisible inks" which will appear under a black light. Hidden text and "micro" text are some other examples. Last is Forensic VSE's. Just like covert VSE's, but much harder to detect — and to counterfeit. This typically entails the use of nano-text.

Defcon used an overt VSE, obviously. They do this every year. The objective was to create an overt VSE which is easy to authenticate, but difficult to duplicate. Given the limited time span of Defcon, it's conceivable that they were aware of this situation, but accepted the risk factor. Either way, they failed with the implementation of their VSE. It was easily overcome with a $1 can of spray paint. That sounds bad no matter how you word it.

Now, it was all a matter of finding some of that paint I keep talking about. Have you ever tried to find a can of paint in Las Vegas? It sounds easy, doesn't it? However, I had no idea where to look. I didn't learn about the street vendor with the paint until much later, but I was still able to pull off nearly the same exact hack. I don't really consider this a hack, but more of a type of social engineering. Who really wants to argue over the difference, though? Suffice to say, SE is a type of hacking. I believe most readers would agree with that sentiment.

I asked David and Carl if they could go find some red paint. After I explained what was on my mind, they wandered off and I didn't see them for another 3 hours. Later that evening, I found them hanging out with Alex from Blacklisted 411 Magazine. I asked if they had any luck and they quickly produced a can of spray paint from one of their backpacks. I was jazzed! They mentioned that they had bought it at Wal-mart and it was "really cheap."

When I got back to our room, I didn't waste any time. I pulled apart my badge (yes, I brought my tool kit with me. Complete with soldering iron), painted it up on both sides and let it dry. I reassembled, checked that it still functioned and set it aside. As promised, I painted up Dave and Carl's badges, too. A little while later I caught myself staring at the badges. I was daydreaming about all the possible situations I may possibly get myself into. Anything from getting kicked out to receiving a pat on the back. Honestly, I had no idea what to expect if I got caught. I sucked it up and ventured out.

Skipping ahead, I found the secure goon entrance very quickly. How could I have possibly missed it? I was able to walk right by the "guard" without incident. It worked! Could it be that simple? I kept telling myself that they knew I wasn't supposed to be there and they were just fucking with me. Just waiting for the right moment to snare me. For

the first 30 minutes or so, I was worried about it. As time passed, I slowly found my comfort zone and eased up on the worries. I began to open up and socialize with the other goons, trying to collect as many names as possible. Nobody seemed to suspect a thing and everyone was very open with me the entire time. I wanted to take some pictures of a few things, but I felt that it may appear too suspicious. I didn't see anyone else taking pictures, so I followed their example. After maybe an hour of wandering around in the backstage area, talking to various goons and enjoying the fact that I was getting away with something otherwise unheard of, I became bored with my new found free-pass and decided to bail out.

The next day, I brought Dave and Carl with me and we slid right by the guard again without incident. I showed them around and introduced them to several of the goons I met the day before, all who shall remain forever nameless. My buddies were obviously nervous. No doubt it was because they were up so close to the goons. I played off of their terror and poked some fun at them. Sorry Dave, I couldn't help it. I explained that it was their first year and they were a bit overwhelmed. The statement was reasonable and nobody questioned it.

During my time in the restricted areas, I had an opportunity of seeing a real goon badge up close a few times. I realized that my painted badge was several shades too dark. Nobody else seemed to notice it, though.

While I applaud Defcon and Joe Grand of GrandIdeaStudios.com for their efforts in trying to make a unique badge for this year—which they did succeed in doing, I can't help but be saddened that they overlooked what I consider to be the most basic physical security principles. Yeah, make it easy to authenticate, but come on. All it took was $1 and a little of my time to open up the doors. I understand that cost is a major factor in the production of something like this and I realize that they were most likely aware of the possible risk and decided to accept that risk. No harm was done, it was only a learning expedition. However, I would suggest that the next DC goon badge implement more security features. The least costly method would be to use a different shape/size or go with a material which doesn't lend itself to being so easily re-colored. Of course, anything can be bypassed with enough determination and time.

I found out at a later point in time that we were not the only ones to have beaten the physical security at Defcon this year. While Hevnsnt had the gonads to report his findings directly to Priest during what was probably the most inopportune moment, we can't make the same claim. We remained anonymous in our activities. Our intent was to provide a proof of concept. I believe we succeeded in our goal. I'd like to state for the record, however, that I did fess up after the event was concluded. Everyone was cool with it. They appeared to treat the breach as trivial. I even got to keep my painted up badge! Thanks for being so cool, guys.

Defcon is an awesome event. I can't wait to see everyone there next year.

SMART CARDS 101

BACK TO HARDWARE HACKING BASICS

Written by: Zachary Blackstone

Have you ever started what would otherwise be a simple hardware project only to find yourself deep in the middle of a journey through hardware hacking? It happens to me a lot more often than not. In fact, it happens to me so often, I've gotten into the habit of taking step by step notes and photographs along the way. It's a good idea for a many reasons. I'm going to share my latest experience with you because I thought it was somewhat interesting. I'd like to mention that I went overboard in my "testing" before doing any actual hardware hacking. I only *partially* did this for presentation purposes.

So, let's roll back three years. No, let's go back even further. Motorola was plugging away, producing a smart card system for various commercial uses. Their Smart Information Transfer (SIT) division was bought by Atmel in 1999. At the time, all of the smart card technology assets of Motorola passed onto Atmel. A few years later, a few Motorola offices throughout the U. S. closed up shop. One such office happened to be [relatively] close to the Blacklisted 411 Magazine offices. Being that the staff of BL411 are a bunch of technology junkies, we had an opportunity of looking over the assets of the office in question before they (Motorola) brought in the trash man to haul everything off to the dump.

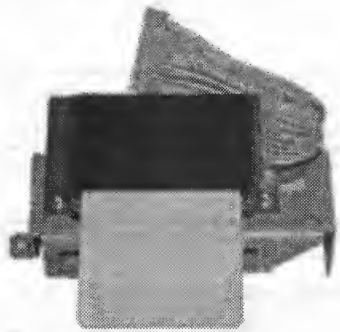


Figure 1 - X2 Coolsat Card Reader.

Typical of a office shutdown, there were plenty of cubicles, desks, chairs, shelving, components, paperwork, phone systems and various other office knick knacks up for grabs. It was a free for all. Luckily, we were one of the first to the scene, so we had first dibs on most of the items others might overlook - programmers, internal memorandum, tech notes, technologies of all types, etc. However, we found one interesting stash we hadn't conceived. Piled away in one room was the remnants of their former SIT division's latest project. It was a fully manufactured Smart Card. No, not just the smart chip. Rather, a smart chip embedded within a credit card sized (CR-80) plastic card. And I'm not saying there was only one of these. Try "hundreds-of-thousands" on for size. First thought at the time was, "cool, they're free so let's take 'em all!" And take all of them we did. Thank you Motorola!

Ok, fast forward to 2006. Early this year we introduced the first-ever hacker membership card to our subscribers. It was met with an overall warm response. Ok—that'll do. So, I've been considering my options for a new membership card for the 2007 year. I've thought about doing another one made from stainless steel just like the 2006 model. I've considered producing them from brass or maybe even aluminum. I was sitting at my desk three days ago thinking about this topic yet again, while I was browsing the internet for something interesting to occupy my thoughts before everyone else arrived at the office. Low and behold, I stumbled upon the free to air (FTA) satellite receivers again (a subject for another article, perhaps). I really dig the X2 Coolsat 6000 model., so I began my standard search pattern. Check google, check ebay, take notes and compare. I immediately noticed the X2 Coolsat Smart Card Readers (figure 1). At that moment, it occurred to me that we still had those smart cards in the warehouse—somewhere. I dropped everything and proceeded to recover those cards.

After an hour of collecting dirt and dust on my brand new Hack the System shirt while digging through shelving unit after shelving unit, I located the MIA cards. I grabbed a small box of 1000 cards and brought them back to my desk. I pulled out a handful of them and started taking mental notes about the physical characteristics of the card. I immediately noticed a small anomaly—at least what I considered to be a possible problem. The pad layout of the smart device didn't look quite right. It appeared to have 10 solid pads (figure 2). We all know that ISO 7816 (the standard by which all smart cards are designed) specs out an 8-pin pad. Hmmm. I began my search for tech docs on the smart card. A brochure, a tech spec doc from Motorola... from Atmel. A photograph of the card from any other source on the net. Nothing.

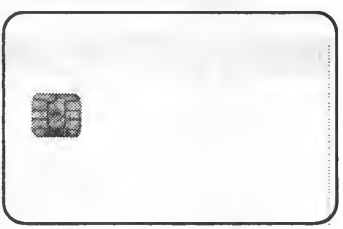


Figure 2 - Smart Card with 10 pin layout.

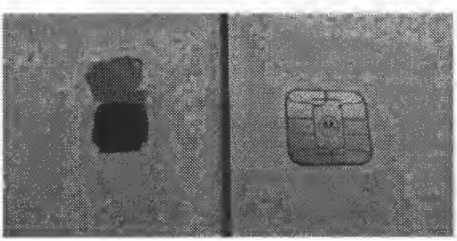


Figure 3 - Smart chip exposed, no markings!

I decided to do some destructive testing of the card. The first sacrificial lamb was stripped of the plastic backing (behind) the smart device (figure 3). My intent was to expose the chip inside of the card and find the identifying chip part number. After taking a blade to it, the plastic didn't put up any notion of a fight. It was clear, however, that there was no markings of any kind. I went a step further and separated the chip from the gold pad leads, hoping I could discover something useful. I was successful in this attempt. Not only did I learn that the chip was well connected to the gold leads I was trying to remove it from, but I also noted that the chip had 6 connections. ISO 7816 only utilizes 6 signal/power lines. Ok, so I had a little more info. It was starting to add up.

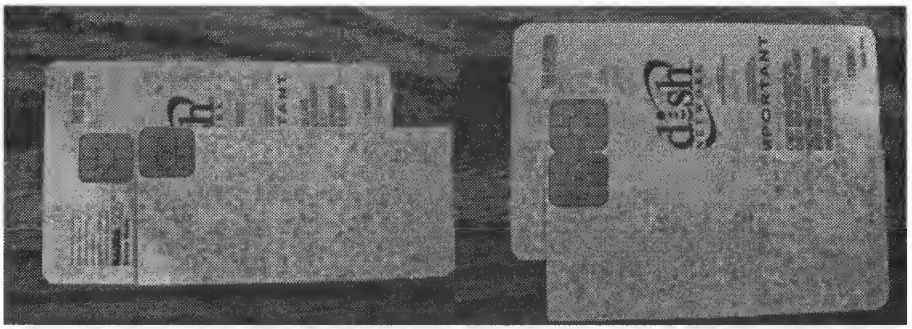


Figure 4 - Photo on left clearly shows that the Smart Chip (SC) is offset slightly higher than a standard ISO 7816 sample card.. Photo on right shows that both chips are placed in identical horizontal locations.

Additionally, I cut up a few more cards, trimming away two sides of plastic away from the card so I could compare the pad layout to a known 7816 compliant card (Dish Network access card). See figure 4. What I found what that the spacing was off ever so slightly. Essentially, the middle six pins appear to line up within a 7816 socket, but the outer four pins don't quite cut it. I marked the card accordingly with the corresponding pin designations. I'll check that later. I also noted a few wires around the outer edges of the card when I cut them. That was unexpected!

Eventually I posted about this topic on the BL411 forum and one of the staff responded with a tidbit that set me in the right direction. Deadpainter (a staff member) suggested that the card looked similar to the Calypso Card (used for fare collection). I checked out the link and immediately focused on the embedded smart device's pad layout. Strikingly similar, to say the least! It too had a 10-pin layout. Ahh, I felt as if I was on the right track. In addition to this I also noted that the brochure mentioned that the card—the 10-pin card—was ISO 7816 compliant. Interesting. It's also ISO14443 (A&B) compliant., which is for a contactless connection, opposed to ISO 7816 for CONTACT connection. So, the card has both contact and contactless standards. I was extremely intrigued by this discovery.

I went back and looked at the card I had cut and noticed that it indeed has a loop antenna embedded within it. It has exactly three loops all the way around. I took the time to determine the layout of the embedded antenna. So, it looks like we have a dual standard card in our grasp. I'll get back to this subject later on in the article.

Ok, now I'm going to backup a little and explain ISO 7816, ISO 14443 and try to get everyone up to speed on the lingo. Overall, it's pretty easy to get a handle on, so you guys shouldn't have any trouble following along. ISO 7816 is an international standard by which electronic cards, in this case smart cards, are described and manufactured. There are several parts to the standard which I will only touch on very lightly.

7816-1, that is part 1, describes the physical characteristics of the standard. It was created in 1987 (yeah, a long time ago) and updated as late as 2003. It describes exposure limitations to x-rays, UV light, EMF and temperature. It goes on to define how far much stress the card should be able to withstand by bending or flexing. Surprisingly, these cards are a lot tougher than you'd think.

7816-2 defines the dimensions and locations of the contacts. This part was created in 1988 and last updated in 2004. It describes the number, function and position of the contacts. A table which identifies the ISO 7816-2 standard is below.

Contact	Designation	Use
C1	Vcc	Power connection through which operating power is supplied to the microprocessor chip in the card
C2	RST	Reset line through which the IFD can signal to the smart card's microprocessor chip to initiate its reset sequence of instructions
C3	CLK	Clock signal line through which a clock signal can be provided to the microprocessor chip. This line controls the operation speed and provides a common framework for data communication between the IFD and the ICC
C4	N/C	No connection. Reserved for future use.
C5	GND	Ground line providing common electrical ground between the IFD and the ICC
C6	Vpp	Programming power connection used to program EEPROM of first generation ICCs.
C7	I/O	Input/output line that provides a half-duplex communication channel between the reader and the smart card
C8	N/C	No connection. Reserved for future use.

I'm going to skim over the next few parts only because they're outside of the scope of this article. 7816-3 describes the electronic signals and transmission protocols. 7816-4 describes the industry commands for interchange. 7816-5 describes number system and registration procedure for application identifiers. 7816-6 describes industry standard elements. It goes on through part 15 which specifies cryptographic functionality.

ISO/IEC 14443 is a four-part international standard for Contactless Smart Cards operating at 13.56 MHz in close proximity with a reader antenna. Proximity Integrated Circuit Cards (PICC) are intended to operate within approximately 10cm of the reader antenna. These proximity "contactless" cards are typically of credit card sized form factor (which is separately defined by ISO 7810—yeah, all this ISO stuff can get confusing). This standard consists of four parts and also describes two types of cards: type A and type B. The difference between the type A and B are with respect to modulation methods.

Part 1 defines the size and physical characteristics of the card. It also lists several environmental stresses that the card must be capable of withstanding without permanent damage to the functionality. These tests are intended to be performed at the card level and are dependent on the construction of the card and on the antenna design; most of the requirements cannot be readily translated to the die level. The operating temperature range of the card is specified in Part 1 as an ambient temperature range of 0°C to 50°C.

Part 2 defines the RF power and signal interface. Two signaling schemes, Type A and Type B, are defined in part 2. Both communication schemes are half duplex with a 106 kbit per second data rate in each direction. Data transmitted by the card is load modulated with a 847.5 kHz subcarrier. The card is powered by the RF field and no battery is required.

Part 3 defines the initialization and anticollision protocols for Type A and Type B. The anticollision commands, responses, data frame, and timing are defined in Part 3. The initialization and anticollision scheme is designed to permit the construction of multi-protocol readers capable of communication with both Type A and Type B cards. Both card types wait silently in the field for a polling command. A multi-protocol reader would poll one type of card, complete any transactions with cards responding, and then poll for the other type of card and transact with them.

Part 4 [ISO/IEC 14443-4:2001(E)] defines the high-level data transmission protocols for Type A and Type B. The protocols described in Part 4 are optional elements of the ISO/IEC 14443 standard; proximity cards may be designed with or without support for Part 4 protocols. The PICC reports to the reader if it supports the Part 4 commands in the response to the polling command (as defined in Part 3).

Ok, now that I've given you a short lecture on the ISO's involved with smart cards, let's get back to the hardware hacking.

Many of the readers would probably ask me, "why don't you just shove the card into a standard smart card slot and see what happens?" Well, anyone who actually knows me, wouldn't bother asking as they know I'm a stickler for the details. I like to research an unknown as much as possible before I dive in. It's all about saving my equipment from certain death. If you've ever taken an electronics class, just think back to the guy in the corner who's projects blow up when power is applied. That guy isn't me. :-)

Now, given the information I have, I'm reasonably certain that middle six pins of MY card will line up with a standard ISO 7816 socket. Next step is to insert the card into a socket which isn't powered up so I can visually confirm pin alignment. Sounds easy, right? By all accounts, it should be a piece of cake to jump through this hoop and move onto the next step.

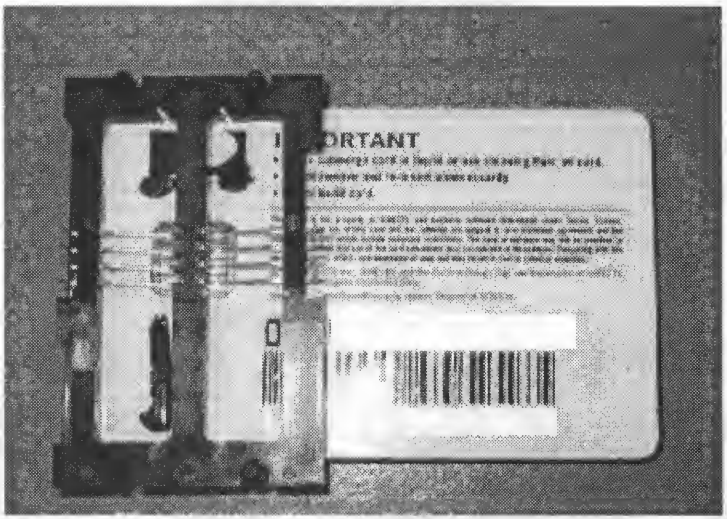
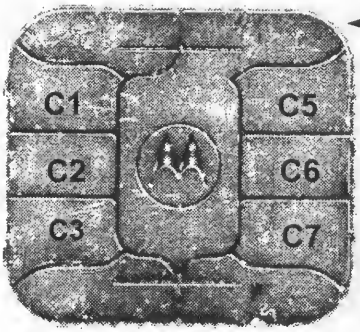


Figure 5 - Example of standard Smart Card inserted into ISO 7816 socket.

If you go back and look at figure 4, you'll notice that the slight difference in height of the placement of the smart device on my card should make a difference when inserted into a socket. I attempted the procedure and just as I suspected, the pins of the socket align perfectly with the middle six pads of the card. However, the top 2 pads and the bottom 2 pads don't align with any of the pins of the socket. The sockets pins C4 and C8 don't mate up with the card, but that's OK since both of those pins are designated "N/C" or "No Connection" anyway. That means they're not used....yet. It appears that C1, C2, C3, C5, C6 and C7 (all necessary for complete connection to a smart card) are actually making contact with the card. This is a very good sign that the card will work in a standard ISO 7816 card reader and encoder.



Shouldn't this be ground?

Figure 6 - Scan of our smart device.

Figure 6 shows a scan of the actual smart chip contacts from my smart card. I've superimposed the contact designations which are derived from where the pins of the card socket connect when the card is inserted. What bothers me is the top right corner, that I've indicated with an arrow. If you look at a normal smart card's contacts, the upper right corner, which is always electrically connected to the middle of the device, is the ground or C5 designation. The fact that the socket places C5 at the contact just below the corner really bothers me and makes me second guess "just plugging it in". Vcc and Gnd across the wrong pins of a device can spell sure destruction of said device. The likelihood of destroying my equipment? Not likely, but possible nevertheless. I need to find some additional evidence that this is the correct pinout . Some specs on the device would be very useful right about now. Chances of me getting the needed documents? Unlikely. Ok, so off to the bench to do some quick comparative testing to determine if I'm on the right track or not.

To further describe the difference between the contacts of the standard ISO7816 and my card, I'm going to draw up a couple of samples of the standard card and my card to illustrate how the connections are being made in the socket.

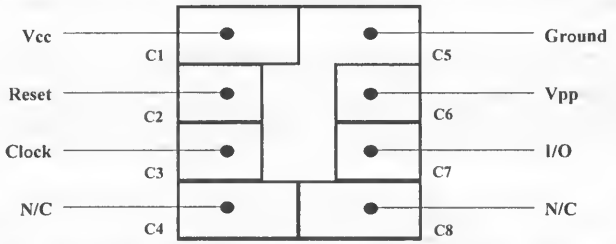


Figure 7 - Standard Smart Card Pinout

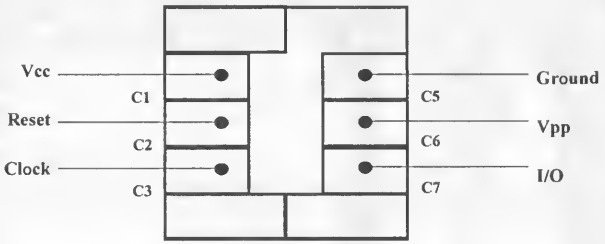


Figure 8 - My Smart Card Pinout

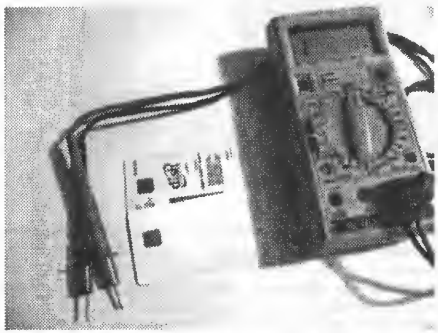


Figure 9 - My extensive testing of the two cards.

What's the easiest way to test for Vcc and Ground? Who needs fancy equipment. Use a multi-meter and check for resistance. You'll almost always get a reading across Vcc/Gnd. Naturally, I have just the tool I broke out my handy dandy Metex multi-meter (it's an old model M-4650 of 80's flavor) and did some quick measurements. First, I checked the satellite card to ensure I was getting a good read off a known Vcc and Ground pair. I then went over to the unknown card and tested across the very top two pins (figure 10). No reading. I then tested across the next two (figure 11). Bingo! Sure enough, the corresponding pins that I designated as C1 (Vcc) and C5 (Ground) above in figure 6 was very likely to be correct. What do the pins above these two do? Not sure yet. I'm not too interested in those pins right now. I'm delighted that it looks like this card may be 7816 compliant for the most part. It may not be compliant with ISO 7816 Part 2 with regard to C4 and C8 not mating up, but that's beside the point.

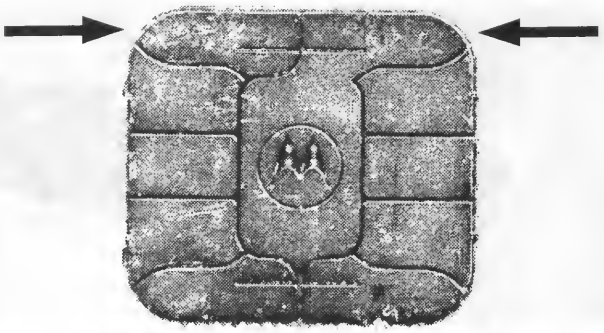


Figure 10 - I first tested across these points. No reading at all. Probably not Vcc/Gnd.

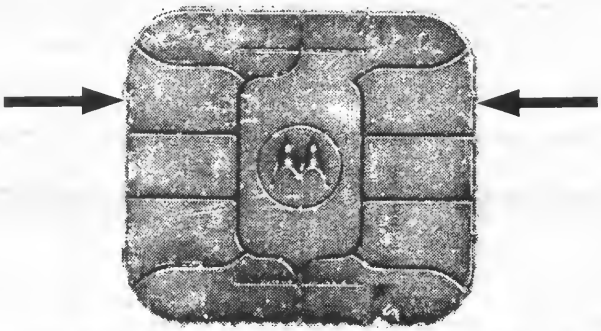


Figure 11 - I then tested across these points. I got a valid reading. Very likely to be Vcc/Gnd.

At this point, I believe it's safe to assume that figure 6 is correct. Now onto the real tests. I'm going to install my smart card reader and try to read one of these cards. Of course, my first thought was to create my own reader. Bargain basement pricing smart card readers are under $20 now, so why bother? Upon closer inspection of my smart card reader, I realize that it's not Windows XP compatible — no drivers for it. Sure, the reader is compatible with ISO 7816-1/2/3 standards and T=0, T=1 microprocessor card protocols, but sadly no XP support. I'm not about to setup a 2000 box for this project. Does anyone even remember Windows 2000? It was awful. Ok, so it looks like it's time for me to shop for a new Smart Card Reader.

Figure 12 - First attempt. SCM Microsystems Model SCR3310 (on the right) and Model SDI010 (on the left). Both appear to support Windows XP and are touted as reader/writer units.

So, after a little bit of research, I decide to try a couple of the SCM Microsystems models. The SCR3310 seems to be well suited for my purposes, but I also picked up a SDI010 because it has "contactless" support. Remember that embedded antenna I found inside of the card? Well, I think it's worth a shot looking into that a little more. And why not, these card readers are relatively inexpensive, plus SCM Microsystems was gracious enough to send us some test subjects on their dime. Thanks guys. You can check them out at www.scmmicro.com

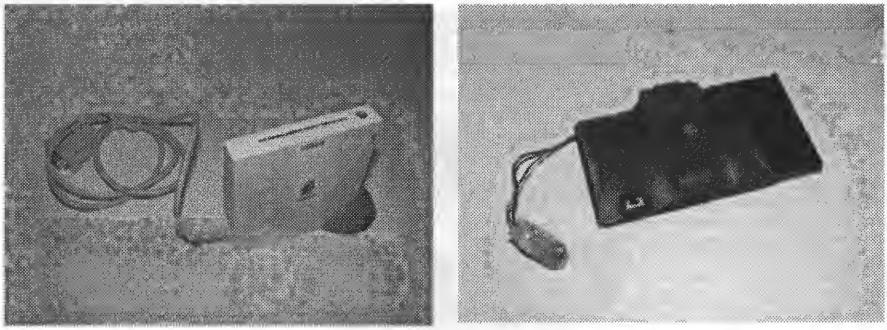


Figure 13 - Second attempt. Gemplus Model GCR410 (on the left) and HackerHomepage "house model" (on the right). Both appear to be decent product, however the old school feel of the house model really does it for me.

Additionally, I spoke with the guys over at Hackers Home Page because when it comes to interesting hardware, they're the place to contact. I told them about the article I was working on and what I was looking for, hoping they'd have some suggestions for me. Not only did they have suggestions but, without hesitation, they sent out a couple sample units for me to play with. The first was their own generic smart card reader/writer and the other was a Gemplus GCR410 universal smart card reader/writer. I can't believe the excellent support I'm getting for this article.

Visit Hackers Homepage at www.hackershomepage.com - they have a very interesting selection of gadgets.

A few days later, I had some packages waiting for me at the office when I stumbled in around 11AM (yeah, had a late night... hey, even the old school hackers like to party). So, yeah, I had some packages waiting for me. Now that's what I like when I show up to work. I thought maybe I had another care package from the dude in NV who always sends us crazy off-the-wall junk. Nope, it was the card readers I had been so anxiously waiting on! I didn't waste any time, I grabbed the boxes and headed to the lab. Once in the lab, I busted out those smart card devices and began to look 'em over.

- At first glance, the Gemplus GC410 really caught my eye. What a nice piece of work it is.
- The SMC Microsystems SCR3310 first appeared to be another run of the mill card reader, but I immediately took note of the classy packaging. Yes, I pay attention to such details. Anyhow, the reader had a good feel to it—definitely a well manufactured item. However, the unit was not bundled with any software which is a drag.
- The SMC SDI010 is a contactless/contact smart card reader. This was packed just as nicely as their other model. However, my first impression of the item was that it was a few notches better than the other model. I couldn't wait to try this one out and see how that contactless mode worked.
- Last reader I checked out was the "generic" unit from Hackers Home Page. At first glance, this one looked a little low-end. But let me tell you something, it was the most interesting of the bunch. The bundled software is pretty slick and looks powerful enough for my needs. Again, looking forward to trying this one out.

I connected the SCR3310 model first. It was a relatively easy install. However, the unit didn't come with bundled software which was a bummer. So, now the search for some generic Smart Card software begins. Where better to start than the SCM Microsystems website.

I visited www.scmmicro.com and immediately found their product driver page. I downloaded the version 4.14 drivers and the V8.06.001 English installer for firmware revision V5.21. Installation was easy and no problems encountered. The device was recognized immediately and everything appeared to be functioning correctly. I checked out the developer tools and utilities section of their website. I was somewhat displeased with the selection of tools, so I went elsewhere.

After only minimal searching, I found ISO7816Prog and SmartCache (www.smartcache.net). Both files are generic software for use with "any" smart card reader. Seems like it might just what I was looking for.

Ok, so SmartCache looks like it might be handy. However, ISO7816Prog proved to be a useless program with no support whatsoever, so I continued my search for another piece of software.

More on this subject later....

After extensive destruction of several cards, I was able to determine the antenna pattern and electrical connections. The antenna consists of three loops of very thin gold wire which is laid out near the outer edge of the card. The antenna has leads running directly into the area of the smart chip. I'm not sure if it's connected to the actual smart chip itself or a secondary chip which is located near the smart chip. While this could be a completely proprietary setup, it's more likely that it's either a 125Khz proximity card or a 13.56Mhz contactless smart card. Given the age, I'm going to go with the 125Khz proximity card type. However, RFID was around in 2003, so it's possible that this could possibly be a genuine contactless smart card running at 13.56Mhz. Only the original docs for this card or physical testing will reveal it's true nature.

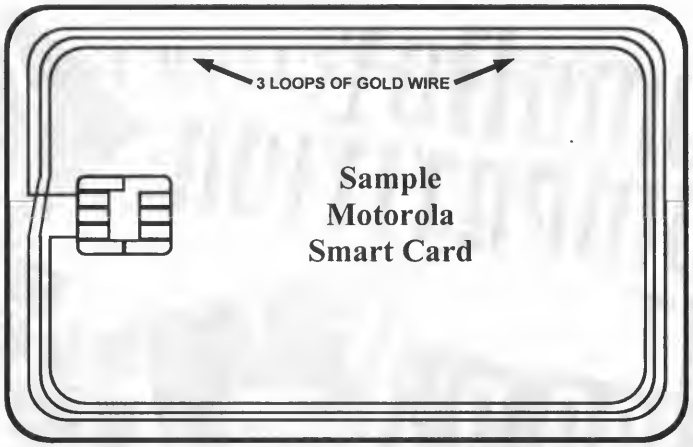


Figure 2 - Smart Card Embedded Antenna.

Since Motorola sold off their SIT division and Atmel doesn't have any idea what I'm talking about, it looks like we're going to have to resort to physical testing. Hey, that's ok. I live for this shit. I'd like to first focus on the older 125Khz proximity "standard" (I put that in quotes because it was a very loose standard) and, if that doesn't work, move forward to the 13.56Mhz contactless RFID/smart card standard. If neither work, it's possible that Motorola came up with their own proprietary design in which case, I'm probably out of luck.

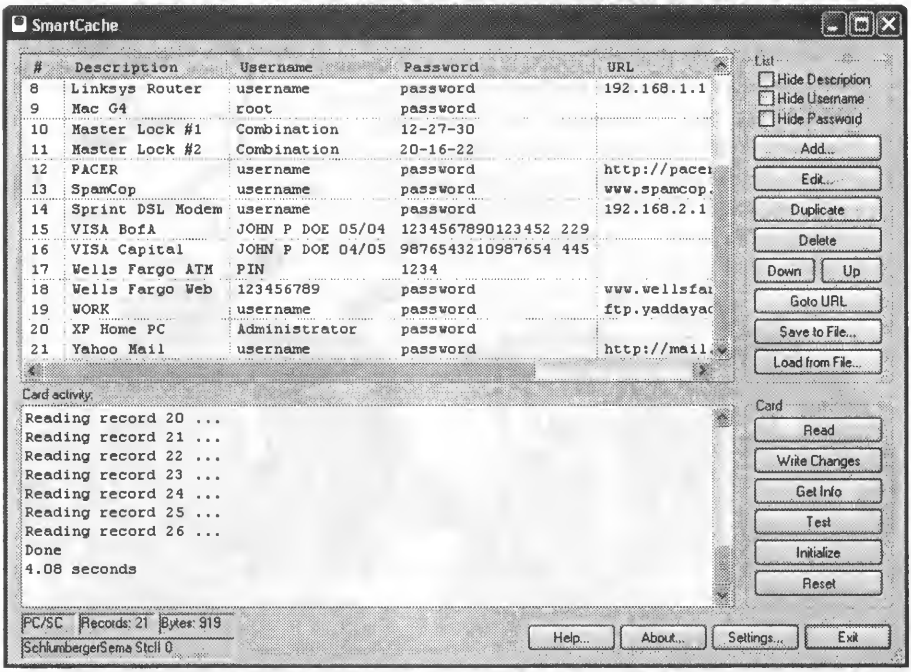


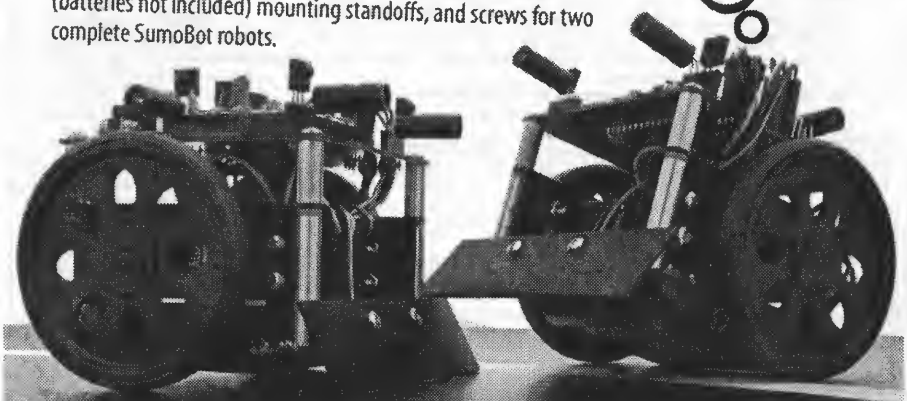
Figure 13 - SmartCache screen shots showing data from a sample file.

Ok, back to software for a minute. After fiddling around with smartcache for awhile, I've decided that I really just don't care for it very much. While it does an OK job of reading the cards, it doesn't offer too much as far as cool features. In fact, I'm having a difficult time locating any decent software for this phase of the article, so I'm going to have to cut the article short while I try to drum up some additional software. So, until next time, keep on hacking.

SumoBot Competition Kit

$199.95

Build and program two high-quality SumoBot robots designed to wrestle in the mini-sumo competition ring (included in the kit)! The electronics consists of a surface-mounted BASIC Stamp 2 module and an array of infrared sensors to detect your opponent and the edge of the Sumo Ring. Additional components include piezospeakers, resistors, pushbuttons and LEDs to build custom breadboard circuits for program mode selection and sensor state feedback. The hardware package includes black anodized aluminum chassis and scoops, servo motors, wheels, 4AA power packs (batteries not included) mounting standoffs, and screws for two complete SumoBot robots.



www.parallax.com

PARALLAX INC.

SURPLUS SOURCES

Your Electronic Hobby / Repair Source list

Here's a small list of new and surplus electronics sources you may find useful if you're trying to build a project or repair a piece of equipment. We've done business with all of these companies and personally recommend them to anyone. Don't forget to mention where you heard about them. If you want a company listed, contact us.

Action Electronics
1300 E Edinger Ave # B, Santa Ana, CA 92705
(714) 547-5169
http://www.action-electronics.com/

Active Surplus
347 Queen Street West
Toronto, M5V 2A4 CANADA
(800)465-5487 (416)593-0909
http://www.activesurplus.com

Active Electronic Supplies Depot
2015-32nd Avenue N.E.
Calgary, Alberta, Canada T2E 6Z3
(403)291-5626
http://www.active-tech.com

Active Electronic Supplies Depot
6029-103rd Street
Edmonton, Alberta, Canada T6H 2H3
(780)438-0644
http://www.active-tech.com

Active Electronic Supplies Depot
1350 Matheson Blvd. Unit 2
Mississauga, Ontario, Canada L4W 4M1
(905)238-8825
http://www.active-tech.com

Active Electronic Supplies Depot
6080 Metropolitain East
St-Leonard, Quebec, Canada H1S 1A9
(514) 256-7538
http://www.active-tech.com

Active Electronic Supplies Depot
5349 Ferrier
Montreal, Quebec, Canada H4P 1M1
(514) 731-7441
http://www.active-tech.com

Active Electronic Supplies Depot
1023 Merivale Rd.
Ottawa, Ontario, Canada K1Z 6A6
(613) 728-7900
http://www.active-tech.com

Active Electronic Supplies Depot
1990 Jean-Talon St. North Suite 109
Ste. Foy, Quebec, Canada G1N 4K8
(418) 682-1130
http://www.active-tech.com

Active Electronic Supplies Depot
3790 Victoria Park Ave Suite 100
Toronto, Ontario, Canada M2H 3H7
(416) 498-9886
http://www.active-tech.com

Active Electronic Supplies Depot
3695 East 1st Ave
Vancouver, British Columbia, Canada V5M 1C2
(604) 654-1057
http://www.active-tech.com

Active Electronic Supplies Depot
106 King Edward St. East
Winnipeg, Manitoba, Canada R3H 0N8
(204) 786-3131
http://www.active-tech.com

Advanced Component Electronics
1534 Berger Dr. San Jose, CA 95112
(408) 297-1383
http://www.acecomponents.com

Advanced Computer Products
1310 E Edinger Ave # A, Santa Ana, CA 92705
(714) 558-8813
Http://www.acpcomponents.com

All Electronics Corp.
P.O. Box 567, Van Nuys, CA 90408
(818) 904-0524
http://www.allcorp.com/allcorp/

Alltech Electronics
1300 E Edinger Ave # D, Santa Ana, CA 92705
(714) 543-5011
http://www.malltech.com/

Alltronics
2300-D Zanker Rd. San Jose, CA 95131
(408) 943-9773
http://www.altronics.com

American Design Components
400 Country Ave., Secaucus, NJ 07094
800-776-3800

American Science & Surplus
P.O. Box 1030, Skokie, IL 60076
(847) 647-0010
http://www.sciplus.com

American Science & Surplus
5316 N. Milwaukee Avenue
Chicago, IL
(773)763-0313
http://www.sciplus.com

American Science & Surplus
33W361 Route 38 (1/4 mile east of Kirk Road)
West Chicago, IL
(630)232-2882
http://www.sciplus.com

American Science & Surplus
6901 W. Oklahoma
Milwaukee, WI
(414)541-7777
http://www.sciplus.com

Ax-Man Surplus
1639 University Avenue
St. Paul, MN 55104
(651)646-8653
http://www.ax-man.com/

Ax-Man Surplus 2
1071 East Moore Lake Drive
Fridley, MN
(612)572-3730
http://www.ax-man.com/

Ax-Man Surplus 4
8008 Minnetonka Dlvd.
St. Louis Park, MN
(612)935-2210
http://www.ax-man.com/

B. G. Micro
555 N. 5th Street, Suite 125 Garland, TX 75040
(800) 276-2206
http://www.bgmicro.com

Ball Electronics
2960 W Ball Rd, Anaheim, CA 92804
(714) 828-1310

Bob Roberts
bob147@bellsouth.net
http://www.dameon.net/BBBB/parts.html

Boeing Surplus Sales
20651 84th Avenue S.
Kent, WA
(425)393-4065
http://www.boeing.com/assocproducts/surplus/retail/

C & H Sales
2176 E. Colorado Blvd., Pasadena, CA 91107
(800) 325-9465
http://www.aaaim.com/CandH/

Cal's Computer Warehouse
3083 Grandview Hwy
Vancouver, BC V5M 2E4
(604)437-5551
http://www.goseecal.com

California Electronic & Industrial Supply
221 N Johnson, El Cajon CA 92020
(619) 588-5599
http://www.californiaelectronic.com/

Circuit Specialists
P.O. Box 3047, Scottsdale, AZ 85271-3047
(800) 528-1417
http://www.cir.com

Davilyn Corp.
13406 Saticoy St.
North Hollywood, CA 91605-3475
(800) 235-6222 (818) 787-3334
Http://www.davilyn.com

DC Electronics
P.O. Box 3203, Scottsdale, AZ 85271-3203
(602) 945-7736
http://www.dckits.com

DIGI-KEY Corporation
701 Brooks Avenue South, Thief River Falls, MN 56701
(800) 344-4539
http://www.digikey.com

Edlie Electronics
2700 Hempstead Tpke., Levittown, NY 11756-1443
(800) 645-4722
http://www.edlieelectronics.com/

Edmund Scientific
101 E. Gloucester Pike, Barrington, NJ 00807-1380
(609) 573-6250
http://www.edsci.com

Electronic Goldmine
PO Box 5408 Scottsdale, AZ 85261
(800) 445-0697
http://www.goldmine-elec.com/

Electronic Materials Recovery, Inc.
3102 W. Thomas Road, Suite 902 Phoenix,AZ 85017
(602) 272-3200
email: emcphx@xroads.com

Electronic Surplus Inc.
5363 Broadway Ave., Cleveland, Ohio 44127
(216) 441-8500
http://www.electronicsurplus.com/

Electronics Warehouse
2691 Main St, Riverside, CA 92501
(909) 686-6186
http://www.the-ewarehouse.com/

Ford Electronics
8431 Commonwealth Ave, Buena Park, CA 90621
(714) 521-8080
http://www.fordelectronics.com/

Future-Bot Components
203 N. Pennock Lane, Jupiter, FL. 33458
(561) 575-1487
http://www.futurebots.com/

H&R Company, Inc.
353 Crider Avenue, Moorestown, NJ 08057
(856) 802-0422
http://www.herbach.com/

Halted Specialties Co. (HSC)
3500 Ryder Street, Santa Clara, CA 95051
(800) 4-HALTED
http://www.halted.com/

Hi-Tech Surplus
605 #. 44th St., Boise ID 83714
(208) 375-7516
http://www.hitechsurplus.com

Hoffman Industries
853 Dundee Ave., Elgin, IL 60120
(847) 622-8201
http://www.hoffind.com

Hosfelt Electronics
2700 Sunset Boulevard Steubenville, OH 43952-1158
(800) 524-6464
http://www.hosfelt.com

International Components Coporation
1803 NW Lincoln Way, Toledo OR 97391-1014
(800) 325-0101

Jameco Electronics
1355 Shoreway Road Belmont, CA 94002-9864
(800) 831-4242
http://www.jameco.com

JDR Microdevices
1850 South 10th Street San Jose, CA 95112-4108
(800) 538-5000
http://www.jdr.com

JGL Components, Inc.
455 Aldo Avenue, Santa Clara, CA 95054
(408) 980-1100
http://www.jglcomp.com/html/index.html

Johnson Shop Products
P.O.Box 160113, Cupertino CA 95016
(408) 257-8614

Just In Time IC-s
4450 Enterprise St #113, Fremont, CA. 94538
(510) 490-1377
http://www.batnet.com/justintime/xtal.html

Kelvin Electronics
7 Fairchild Ave, Plainview NY 11803
(800) 645-9212
http://www.kelvin.com

Mark Capps
1842 Chrysler Dr Atlanta, GA 30345
catfishh@bellsouth.net

Marlin P. Jones & Assoc.
P.O. Box 12685 Lake Park, FL 33403-0685
(407) 844-8764
http://www.mpja.com

MCM Electronics
650 Congress Park Dr., Centerville, OH 45459-4072
800-543-4330
www.mcmelectronics.com/

Mendelson Electronics
340 E First St Dayton, OH 45402
(937) 461-3391
http://www.meci.com/

Mouser Electronics
958 North Main St. Manfield, TX 76063
(800) 346-6873
http://www.mouser.com

MWK Industries
1269 W. Pomona, U112, Corona, CA 91720
(909) 278-0563
http://www.mwklasers.com/

Ocean States Electronics
PO Box 1458, 6 Industrial Drive, Westerly RI 02891
(800) 866-6626
http://www.oselectronics.com

Orvac Electronics
1645 E Orangethorpe Ave, Fullerton, CA 92831
(714) 871-1020

R-Vac electronics
23684 El Toro Rd # O, Lake Forest, CA 92630
(949) 586-1210

RA Enterprises
2260 De La Cruz Blvd., Santa Clara, CA 95050
(408) 986-8286
http://www.angelfire.com/free/proto.html

Sav-On Electronics
13225 Harbor Blvd, Garden Grove, CA 92843
(714) 530-0555

Skycraft Parts & Surplus Inc.
2245 West Fairbanks Ave, Winter Park, FL 32789
(407) 628-5634
http://skycraftsurplus.com

Surplus Sales of Nebraska
1502 Jones St., Omaha, NE 68102
(402) 346-4750
www.surplussales.com

Surplus Shed
8408 Allentown Pike, Blandon, PA 19510
(877) 7-SURPLUS
http://surplusshed.com/

SURPLUS TRADERS
PO Box 276, Alburg, VT 05440
(514)-739-9328
http://www.73.com

Unicorn Electronics
1142 State Route 18 Aliquippa, PA. 15001
(800) 824-3432
http://www.unicornelectronics.com/

Vetco Electronics
12718 Northrop Way
Bellevue, WA 98005
(425)641-7275
http://www.vetcoelectronics.com/

Weird Stuff Warehouse
384 W. Caribbean Dr., Sunnyvale, CA 94086
(408) 743-5650
http://www.weirdstuff.com

DUMPSTER DIVING

The talent of digging up valuable items from a heap of garbage

By Trash-00X

You may have heard the term "dumpster diving" a few times and wondered to yourself what it's all about. It's easy to imagine it as a sport of some kind where someone jumps off a roof into a dumpster. I mean, there have been much more crazy "sports" out there, so why not? Maybe, but that's not what it is. In fact, dumpster diving isn't really a sport but rather a way of living. In a nutshell, dumpster diving is nothing more than the act of digging through the trash. I'm sure you know what a "trash digger" is, right? Dumpster diving is what a trash digger does, most likely to make a living or to obtain something with perceived value for no cost at all.

According to the dictionary jargon file, Dumpster Diving is defined as:

"The practice of raiding the dumpsters behind buildings where producers and/or consumers of high-tech equipment are located, with the expectation (usually justified) of finding discarded but still-valuable equipment to be nursed back to health in some hacker's den. Experienced dumpster-divers not infrequently accumulate basements full of moldering (but still potentially useful) cruft."

Ok, but digging in the trash to make a living?! What, are dumpster divers bums or something? Not really. While you'll find your average bum, hobo, transient, etc digging in the garbage for food, clothing or cans to recycle, this isn't the same breed of people we're going to talk about in this article. We're going to focus on the people who seem normal (ie: have a job, money, a home and most like a family as well) and find it worth-while to hop into the trash....for some reason.

Face it, a lot of people find value in other people's refuse. One person may believe something to have no value while another believes differently. This concept is what has made the idea of dumpster diving become so popular. In fact, it's such a popular subject, that there are websites devoted to the topic. Now, that's pretty amazing.

Ok, so let's get on with the article.

One day, you might come along a dumpster such as the one pictured to the right. "Yeah, so what?" you may think to yourself. It may seem just like any other dumpster, but what makes this one so different from your run of the mill dumpster is the fact that there's some hidden value in this otherwise plain looking garbage. The lay person would never notice this, so don't feel bad.

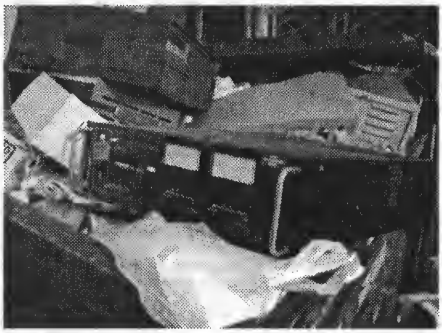
The experienced dumpster diver would immediately recognize the obvious electronic equipment sitting on the top of the heap as being somewhat valuable. This would normally be enough to persuade further investigation (ie: digging a little deeper). Upon a detailed inspection of the contents of this dumpster, the number of valuable items obtained was large. The final results were quite staggering and a real eye opener.

Gathered up were about two dozen pieces of equipment total. A quick look on ebay proved to get an initial valuation of the equipment at roughly $200. The items were cleaned up, tested, and listed on ebay (some listed "as-is" because they did not function). I know, most people who read Blacklisted! 411 probably don't like to use ebay, but for the purpose of demonstrating "value" for the sake of a timely completion of this article, I decided to offload the items in this fashion to get quick results. So, the final tally once everything sold on ebay (everything was listed 3-day with no reserve) was over $700! To be honest, I was surprised by the total income from the material. Everyone paid and the items were sent out. Done deal.

The point is, the garbage found in this one specific example generated over $700 on the open market. Dumpster diving truly is a way to make some money, either on the side or for a full time living if you can handle it. Yes, these are ebay

prices, but it's only one example of how this kind of find can be later sold to generate some decent money.

WHERE SHOULD I LOOK?



Where can you find scores such as the one described in this article? All over the place! However, I'll try to help guide you a little bit so you can find your own treasure trash.

Mainly, you will find these kind of dumpsters (the ones filled with cool junk) behind industrial business centers. You'll also find them being manufacturers of electronics and computers, but their trash tends to be locked up and inaccessible. One of the most overlooked places are the dumpsters behind THRIFT STORES - they toss a lot of stuff they don't think they can sell (you can find a lot of old computers and game consoles here). You can also check electronic/computer store dumpsters, bookstore dumpsters and video rental dumpsters. They all usually have something worth grabbing. If you're not sure, look in the local phone book for places such as the above and get their address. Go there and take a peek in their trash. It can't hurt.

IS IT LEGAL TO LOOK THROUGH SOMEONE ELSES TRASH?

Some cities and counties have laws against digging in the trash, so your best bet would be to ask the people/company who dumped the trash if you can have it. If they agree, there's no issue of possibly breaking the law to deal with. If they say NO and you dig anyway, there's a good chance you'll get in trouble. You can take your chances, but remember, ignorance is no excuse for breaking the law. Be careful and check with your local city ordinances on the subject. Don't trespass and don't steal. Follow this and you should be fine.

IS THERE ANYTHING I SHOULD DO OR A CODE OF ETHICS?

Use some common sense and clean up any mess you may make during the process of a dumpster dive. In fact, even if you don't make a mess and there happens to be a mess near the dumpster you're diving into, clean it up anyway to avoid being blamed for it. Naturally, if you have to dig deep, you're going to end up making a mess. Clean it up when you're done! If anything, this will help to ensure the dumpster will not be fenced in at a later date. If there's a fence surrounding the dumpster, don't climb over it. The fence was put there for a reason, so respect it's limit.. If you hurt yourself during a dumpster dive, don't sue the owner of the trashcan since you went out of your way to get into the dumpster in the first place. Oh, and don't take the name "dumpster diving" literally - in other words, don't actually "dive" into the dumpster! Climb in, carefully.

WHAT SHOULD I BRING OR WEAR?

A vehicle is usually a good start, but you should at the very least have a bag or a box to contain any findings you may come across. Be sure you wear long pants and avoid wearing shorts. Bring some gloves as well. Further, you may wish to bring a bottle of water (or a key for a water faucet - a lot of business centers have faucets with no key on them) so you can wash your hands and a bottle of hand sanitizer. Try not to dress like a ninja (in all black) and dumpster dive at night - it looks too conspicuous and people will make complaint calls to the police. Bad idea.

WHAT KIND OF STUFF CAN I FIND?

It's fairly easy to assume you will be able to locate any of the following if you look enough:

Computers, televisions, stereos, VCR's, DVD players, CD players, telephones, answering machines, electronic components, wire, test equipment, magazines, books, software, furniture, and many other items of value.

What's somewhat interesting is that a lot of the electronic/computer "reclamation" centers around today started with a guy digging in the trash. No, seriously! I can name at least three VERY well known places in the area which started this way. There's still plenty of room for this cash-cow to spit out money for new people getting started.

In closing, all I have to say is ENJOY YOUR DUMPSTER DIVING!!

SOME INTERESTING WEBSITES TO VISIT:

http://www.frugalvillage.com/dumpsterdiving.shtml
http://www.dumpsterworld.com/
http://www.phonelosers.org/dd.html
http://members.aol.com/TheDumpsterLady/thedumpsterlady.htm
http://mytrashy.com/
http://www.goddessofgarbage.com/
http://www.allthingsfrugal.com/dumpster.htm
http://www.thelivingweb.net/dumpster_diving_for_fun_and_profit.html
http://www.angelfire.com/ks/mcguirk/dumpsterdiving2.html
http://www.net4tv.com/voice/story.cfm?storyid=3565
http://asuaf.org/~fsgpe/dive.htm

SALVAGE HOUND

THE ART OF LOCATING QUALITY SALVAGE ITEMS

By TechnoHeap

Greetings fellow collector. I have been collecting, buying and reselling integrated circuits (otherwise known as "chips"), electronic parts and equipment since the early 1980's. In the time that I have been doing this, I have grown to know first hand many sources who deal in LESS THAN WHOLESALE priced chips, computer equipment, electronic equipment and parts. That's right, these items are available for pennies on the dollar and this is literally, not figuratively speaking. Some of the things you will be able to find at rock bottom prices: Intel, AMD, NEC and DEC gold chips, MacIntosh computer equipment, EPROMs, EPROM programming equipment, vintage computers, chips, parts, newer equipment, computer parts, brand new excess inventory chips...the list goes on and on.

Have you ever wondered about those $300 - $400 Intel C4004 chips for sale on ebay and wonder to yourself how much you could get them for if you knew the sellers source? How does $40 per POUND sound to you? It takes quite a few of these chips to add up to a pound, so you can see the potential. The going rate for "gold" chips is in the range of $20-$45 per pound and you can buy this stuff all day long at those prices... IF you know where. The sources I will reveal generally don't care what the chips are, only their bulk value. This is where a person with the right knowledge can make a killing regarding resale of the same items.

I've seen these sources come and go by the dozens over the years. What few of these sources remain have been a very well kept secret among the few in the know and to my knowledge, nobody has ever revealed these sources in an all in one information article before. What is about to be revealed to you isn't "fluff" like a lot of other informational articles or those "e-books" provide, you know the ones that claim they're going to reveal wholesale sources to you and you end up finding out it's just a bunch of useless, and I use this term loosely, information. Anyhow, the information I will provide you with is specific hardcore rock bottom priced sources which other people use to obtain the parts they resell - even EBAY sellers! You can use this information right now and make money immediately! Furthermore, it won't break your wallet to stock up on some parts for immediate resale....or collecting.

I'm officially out of the chip/equipment collecting/buying/selling business and since this highly secretive information no longer serves my needs, I'm going to spill the beans once and for all which will allow a whole new generation of collectors and entrepreneurs to access the massive opportunities us old-timers have had all to ourselves for decades. Are you ready? Be sure to check out each and every single one of these places and BUY, BUY, BUY as much as you can -- stock up and resell until you're blue in the face. Don't forget where you got this information, either -- a simple letter to Blacklisted! 411 telling them about the great deals you've found for yourself will do. I'm going to be listing salvage yards, obscure retail locations and swapmeet sources. These are all worth the time to visit and explore.

First on the list is a favorite of mine:

SILICON SALVAGE
1500 N. DALE STREET
ANAHEIM, CA 92801
TEL (714)523-2425
FAX (714)523-2552
EMAIL: sales@siliconsalvage.com
URL: http://www.siliconsalvage.com
EBAY ID: SSINC1500

Type: Salvage Yard/Excess Inventory
Contact: Chuck Hulse
Alternate Contact: Dan (VERY cool guy)

This is by far the most interesting salvage yard of them all. Not only are they huge, but they have a very wide variety of stock to choose from. The down side to this place is that they're very aware of EBAY and have started to price their items based on what they *might* get for it on EBAY. There's still room to haggle, so don't give up on this one. They're a bit on the moody side as well. One day they might be your best friend in the world, the next you might be treated like they never saw you before. It doesn't matter how much money you spend at this place, you're just another customer. Try to remain calm and friendly at all times (even in the face of apparent rudeness) and flash some money around (I recommend that you stick with cash only at this place). Whatever you do, don't waste their time and be sure to arrive no later than 2:30PM if you want to buy anything. If you want something from them, be prepared to follow through and spend on the spot.

This place has an INCREDIBLE supply of used EPROMS in *excellent* condition (pins real straight, stickers still on them - nothing a little acetone bath won't fix right up). Going price is anywhere from $3/lb to $5/lb for the EPROMs. Purchase them by the 5 gallon buckets. (roughly 55-65lbs per bucket). Generally, the more you buy, the cheaper per pound rate you'll get. You won't find a better deal on better quality used EPROMS than this place! They also have a great selection of overstock components, sometimes still in the rails - be prepared to pay a bit of a premium on these (whatever they feel like charging you that day). Whatever the price, you'll still be getting a killer deal on the components. This place has a fully functional scrapping business going on each and every weekday - what this means is you will have access to incredible amounts of recovered chips....if they're not recovering them already, tell them what you're looking for and how much you'll pay for them (if ceramic/plastic, offer $4/lb - $5/lb, if INTEL brand chips, offer $6/lb - $7/lb) and they'll usually start saving them for you. Come back once a month and collect your spoils. This is a great way to stock up on old obsolete 6500, 6800, 68000, Z80 series processors and the support chips. I've found that with a typical purchase from this place, 98 out of 100 chips are typically GOOD functional product. If you want gold plated Intel chips from these people, be prepared to pry some hands. If you're not equipped with the proper information, they'll hmm and haw and play the price dance with you. Just be prepared to spend $40/lb and offer it right from the start. Things will go more smoothly once you do this. Trust me.

If you're looking for laser equipment, this place usually has an interesting supply of such material. I've seen everything from HeNe's to full blown argon setups complete with power supply, fully functional and CHEAP! I once helped arrange a deal for a friend on a huge load of laser equipment from Silicon Salvage and the entire load only cost $700 -- not bad considering the amount of lasers. The person whom which I arranged the deal for turned the lasers around and made $7000 cash while keeping two of the argon lasers for himself. How's that for some fast cash? Only one dead HeNe in the pile - everything else was top notch product ready to sell.

Do you want hard drives, MacIntosh computers, Silicon Graphics machines, network cards, ram chips or anything else computer related? This is by far one of the largest computer scrappers I have ever seen. Again, pennies on the dollar for GOOD stuff! You will find things like Seagate Barracuda, IBM, Maxtor and WD hard drives, DIMMs, netgear, 3Com and Intel network cards, IDE, SCSI, Fiberchannel, etc. The selection is quite stunning and very impressive.

If you're looking for scrap circuit boards, boy this is the place to be. I found a pile of Tektronix 1240D1 and 1240D2 (9 channel / 18 channel) acquisition cards headed for the grinder. I obtained them for $5/lb. Needless to say, this was an excellent price. I managed to find a couple of P6460 PODs the same day which were thrown in to the pile for free. Wow! I've also found tons of old arcade game circuit boards heading into the same grinder-bound pile. Everything from old Atari Asteroids, Tempest and Spaceduel boards to more rare Cinematronics boards. All were in non working condition, but easily repaired (nothing physically damaged on them). Again, $5/lb. Can't beat that with a stick, I tell ya!

If you're looking for old equipment, they've got that too.... and lots of it. EPROM programmers, o-scopes, multimeters, Huntron Tracker circuit testers, Tek 1241 logic analyzers, they have it... or will have it sometime soon. God, the selection is simply stunning! The equipment comes and goes all the time, so tell them what you want, tell them you'll PAY and give them a way to get ahold of you. Let me give you some for instances. What's the going rate for a Huntron Tracker 2000? How about the Tek 1241 logic Analyzer? How about a Data I/O 29B with LogiPack and Unipack 2B? I found each and every one of these for $25 each at this place. Fully functional and worth every penny! This was a time when the Tracker was going for $700 on ebay, the 1241 was going for $1500 on ebay and the Data I/O was going for a cool $300. Times change and prices fluctuate, but I know you'll get a great deal on anything you buy from these people.

GOLD'N WEST SURPLUS
346 AMERICAN CIRCLE
CORONA, CA 92880
TEL (909)340-1501
FAX (909)340-1504
Email: sales@goldnwestsurplus.com
URL: http://www.goldnwestsurplus.com

Type: Salvage Yard
Contact: Mark Pickering

This one is an oddity. If you walk in the front door, to the right you will find yourself in a retail-style used computer showroom. Don't bother with it. Ask the receptionist if you can check out the yard and warehouse. You may get an OK or they may just ask you what you're looking for - your mileage may vary here. Just so you're prepared, this is what they have. When you walk into the warehouse, the first thing you will notice are racks and racks and racks of old useless POS dot matrix printers. Stay away from this junk. Focus on the circuit board salvaging. They have a full service board scrapping business going on in here. They have the most incredible selection of gold plated chips I have ever seen in a scrap yard. You'll pay $30-$40/lb for these, but you can pick and choose.

I've personally purchased a small pile of white ceramic Intel C4004 and Intel C1702 EPROMs from them for $30/lb. I turned those around quickly and made bank. Another time, I found a handful of C8008 chips and a handful of the super rare G8008 chips for the same $30/lb. The G8008's sold for over $800 each to some very eager collectors! Anyhow, when I was there, I mainly focused on the EPROMs they had for sale at $4/lb - $5/lb which was easy to turn around for $6-$10 per 27C4004 EPROM at the time. While the quality wasn't nearly as good as that of Silicon Salvage, they had a lot to pick and choose from - and you could buy as much (or as little) as you wanted. No "by the bucket" minimums here. The deals are so great though, that you may find yourself buying a bucket or two anyway. Aside from the EPROMs were tons of boards coming through with 68000 microprocessors. I scrapped a few myself and bought them at $5/lb. Every single 68000 was in perfect condition and was tested GOOD. Anyhow, they have boards coming through with all the old 6500, Z80, 6800, 68000 processors as well as 4116, 2114, 6116, 6164 RAM chips. It's a part lovers dream particularly with the low prices. You'll be able to spend days on end digging out those jewels for your own collection. The people are really nice here, but please be forewarned, make all purchases at the front desk and get a receipt!

They scrap a considerable amount of computers here, so it's worth mentioning that you can get yourself an awesome deal on used hard drives, network cards and Pentium class processors as well as scrap value 8080 through 80486 CPU's .

You will also find large amounts of electronic test gear over here. This is usually located in the back yard area and may be swapmeet-bound. If you make the right offer, you can get yourself some serious equipment for cheap. Prices fluctuate severely in this area, so I cannot guide you directly. Offer low, when they make a counter offer, try about 20-30% less than they want as a counter offer to them. It usually works.

This one is simply a "must visit" if you're a chip collector or reseller of collectible chips. Period!

RECOMP GROUP (RECYLCING)
1704 S. SANTE FE STREET
SANTA ANA, CA 92705
TEL (714)542-3144
FAX (714)542-3145
PGR (800)938-7296
Email: greg@recomp.tv
URL: www.recomp.tv
EBAY ID: recomptv

Type: Salvage Yard
Contact: Greg McBride
Alternate Contact: Ed

In a word: EQUIPMENT. You name it, they have it or can get it. Tektronix, Intel, Data I/O, HP, etc. I've seen it all and bought a lot of it for myself. Lots of room to turn a profit on their stuff, even through they're selling on ebay now. They have an incredible supply of printers and run a board scrapping facility much like GoldnWest. Tell them what you're looking for, ask to look around. If you want to stick with gold plated Intel, they got it. If you want EPROMs, they got it. It's a bit difficult to get your foot in the door, so spend some cash on something real quick and then let them know what else you want. They'll perk up when they see some cashflow coming in their direction. If you check out ACP every odd month, these people have a huge display in the back lot right in front of their place. Lots of goodies to look through at great prices, too! Scrap wire (18GA - 22GA) still in spools of several thousand feet available here from time to time for $4 a spool. GREAT deal! If you take the time to dig around at the swapmeet, you'll find some great deals, particularly with old equipment. I've found Hewlett Packard 1631D logic analyzers by the dozens here over the years. $25-$35 each, complete with pods, leads, clips, etc....and WORKING. I've never purchased a non-working unit at this place to date. It's good stuff for great prices! I've also picked up a lot of Intel gear as well - mostly vintage CPU/component evaluation units - for $10-$15 each. These are highly collectible items worth hundreds each on ebay and the open market. It's worth your time to know these people.

PACIFIC SYSTEMS
1505 E MCFADDEN
SANTA ANA, CA 92705
TEL (714)541-4121
FAX (714)541-4858
Email: pacsys@deltanet.com

Type: Salvage Yard
Contact: Ivar
Alternate Contact: Paul Horn
Alternate Contact: (Herman - very cool warehouse guy)

This is a smaller outfit, but very useful if you're looking for specifc equipment. This place has crazy hours of operation. I know they're closed on Friday at 12 noon through the entire weekend. Show up on a weekday somewhere between 10AM through 11:30AM and go to the back of the place (enter through the north-most rollup door) and talk to Herman (he's usually sitting at the desk in the back or pulling something apart). Ask him if you can look around. He'll say, "yes." Now it's time to go dig in. Look around and have at it. It usually takes some digging to find the treasures, but they're there.

This place used to be excellent for monitors (17", 21") NEC, SONY, SILICON GRAPHICS, etc. Then the government decided monitors were hazardous waste product (you know, all the lead, phosphorous, etc) and Pacific stopped collecting these for resale, mostly. It's a shame because the cost for a nice BIG working monitor was CHEAP!! Anyhow, on to what they DO have. Printers - tons of them. Big ones, small ones, b&w, color. You name it, they probably have it or will get it sometime soon. Just a note, they sell their printers (and used to sell their monitors) to a company listed below (Alltech) - you can see what this place sells it for then go to the other place to see how much profit they're making...and they do this every day of the week. $$$ machine, man!!

So, if you're not in the market for a used printer, how about some test equipment or network equipment? I've purchased more Data I/O, Tek and MacIntosh equipment from this place than I'll ever know what to do with. Did I pay much? Nope. $25 each for the Data I/O gear, $20-$50 each for the Tektronix gear, usually $25 each for the PowerMacs. All easy to turn around and double, triple, ten times my money back. You know the drill. This is a wonderful source for Tektronix 1241 units -- most paid was $25 each - complete with PODs, leadsets and grabbers!! You can also find Hewlett Packard 1631D logic analyzers and 16500A, 16700A logic analysis systems for next to nothing. I've never paid over $50 for any of these items. See what they go for on Ebay right now. I've even managed to find EPROM programmers (the top end stuff) over here - Everything from the PSX 1000 and Unisite/Chipsite down to the lower end System 19 and 29B units -- everything under $75 ($25 for the lower end stuff). If you like Fluke, this stuff shows up from time to time as well - everything from the 9010A to the 9100A and every imaginable accessory for these babies. The biggest equipment score here was a HP 1670D for $100. It was working and brought in some serious cash. Look at what these are going for - as-is, untested, etc. $$$$

I once found a small box with over 10,000 Tektronix clips (grabbers) (the kind used with their logic analyzers). All of them were brand new, still in their factory packages. I bought the box for $35. SCORE!!! If you know anything about Tektronix, you know what those clips go for - especially when they're brand new still in the package. The deals like this are many and very similar. This is an excellent source for used APC UPS units. I've picked up a dozen or so used 1250 SmartUPS units for $25 each - working!!

You just have to check this place out from time to time and see what they have. You'll have to make sure Paul or Ivar is there when you're ready to make a purchase. Herman's great and will hold stuff for you, but he can't make any sales - he's just the eyes and ears of the place who keeps it running along. Make sure you get to know him as he's worth it. If you need something, he'll usually know whether they have it or not and where it is.

SCRAPTRONICS
ONTARIO, CA
TEL (714)476-2420

Type: Salvage Yard
Contact: Dean

I've bought many items from this place, everything from computers and chips to equipment and wire. Excellent bottom dollar scapper. The selection isn't as good as the bigger places above, but the prices are about 1/5th of the ones above. I've found working Amiga Toaster 2000 systems for $20, Data I/O Unisite programmers for $15, Data I/O System 29B loaded with extras for $10, etc. The deals are awesome when they come along and this place is definitely worth the mention. You have to visit them a lot to find quantity. This place has moved a lot over the years and I'm not quite sure where they're located now. The place used to be owned by Kevin, then sold to Terry, then sold to Dean. Dean answers the number above and takes orders. Tell him what you're looking for and he'll help you. It's really worth the call.

GLOBAL METAL RECYCLING INC
930 EAST WALNUT STREET
SANTA ANA, CA 92701
TEL (714)547-9079
FAX (714)547-4655

Type: Recycling Center
Contact: George

I wandered into this place one day just out of curiosity. From the outside, it looks just like any other recycling center; people bringing in their cans, bottles and newspaper for $$. Upon a quick scan of the place, I found that they had large bins full of 18GA - 22GA spooled wire - hundreds upon hundreds of spools (3000' - 10,000' spools). I asked around and found the guy in charge. His name is Geroge. He quoted me a price of $0.35/lb on the wire which is GREAT. I bought a few hundred spools and spent some money for the day. This was good stuff, too. Anyhow, I was able to sell the spools for much more than I paid, so I was happy.

The second trip was even more successful. I found more spools of wire, this time it was silver plated Tefzel military grade wire! How much? $0.35/lb!! Needless to say, that was a killer deal! On another trip, I found a few gaylords (large pallet boxes) worth of scrap circuit boards - most likely headed over to Gold'n West or Silicon Salvage. I took a quick look at some boards and found that they were laced with 4116 RAM chips, 2114 RAM chips and tons of gold plated Intel 8080 circuitry and support chips. They wanted $2/lb on the ceramic and plastic RAM chips and $25/lb on the gold plated chips. Done deal! Another purchase for boards cost me $2/lb for high grade! Not bad. Another trip, I picked up 200lbs worth of aluminum heat sinks (mixed, but brand new). I managed to pick 'em up a scrap prices! Anyhow, I've bought from these people maybe a dozen times... each time was an excellent score and the price was just right. Check them out.

A&M METALS INC
2301 W 5TH STREET
SANTA ANA, CA 92701
TEL (714)547-6507

Type: Recycling Yard
Contact: Steven Carr

This is a recycling center. You'll find a lot of people bringing in their cans and old copper pipes for scrap money. Ignore this. What most people don't notice are all the cool items in the back of the yard. There are piles and piles of monitors (some working, some not), piles of old MacIntosh (Apple IIE, Apple IIC, Apple IIgs, Powermacs, etc) computers worth taking the time to scrap for parts. I found a pallet of brand spanking new KEC transistors from this place, the usual 2N3904/2N3906 - 10 crate boxes of each and a ton (roughly 15 crate boxes of two different values) of surface mount transistors (I don't recall the part numbers) all for $100. This was an incredible find as the parts were only 2 months old on the date codes and the parts sold like crazy once I had them. I made $30 a reel on the surface mount parts and $10 per 100 pieces of the 2N3904/2N3906. I never sold all of them (I kept the 2N3904/2N3906 for myself after I sold a few crates worth), but I sure made a lot off this single deal. I've found boxes of wire, boxes of new old stock gel cell batteries, boxes of brand new motors and even metal cabinets with drawers for $20...really NICE stuff. I also found two of the most beautiful metal card cabinets I've ever seen (they work great for storing tubes of chips) - for only $10 each! These were easily $800ea new.

Somewhere along the way, the owner got wise to the art of electronics and computer scrapping and hired Steven Carr to take care of the job. They are now a full on monitor recycling place and they scrap out tons of electronic equipment. If you ask for Steve, he'll show you the circuit boards and other good stuff available. You can get good prices on EPROMs and other socketed components if you're willing to take the time to pull the parts. Expect to pay $2/lb on the high grade circuit boards, $4/lb-$6/lb for plastic/ceramic components you pull from the boards. It's tedious work, but it's worth the money saved!

BG MICRO
555 N. 5TH STREET SUITE 125
GARLAND, TX 75040
TEL (800)276-2206
TEL (972)205-9447
FAX (972)205-9417
Email: bgmicro@bgmicro.com
URL: http://www.bgmicro.com

Type: Retail/Catalog Sales
Contact: None

This is a very cool place. I've done most of my purchases over the phone with them and boy have I obtained some pure gems from them. They do a lot of salvaging and sell what we call "reconditioned" components - that means they're socket pulls. They fully guarantee the parts and the best part is that on any given part you order, you could get plastic, ceramic, white ceramic, gold plated, etc - they only care about the base part number. So, the idea is to ask them for the "gold" or "white ceramic" version of the intel 4004 or 8008 you've been needing so badly. I've ended up with loads of gold plated Intel chips through them for less than retail, but more than my usual wholesale - but it wasn't of any concern when I was able to immediately turn around and sell them for hundreds of dollars per chip to those crazy chip collectors. They may be out of 4004/8008, but you'll probably still be able to find a lot of highly collectible AMD/INTEL chips. Tell them what you're looking for. Be sure to ask for a free catalog from them and download their PDF version to tide you over until the real one arrives. They have a lot of excellent stock and a lot of sources for the parts they don't have in stock. They once had a pile of new old stock Condor brand power supplies for old Cinematronics arcade games. I believe they were $4.95 each. It was a killer deal considering these are impossible to find anymore. They'll surprise you with their selection. Oh yeah, they're extremely friendly and BILL 30-day if you're a good buyer.

ALLTECH ELECTRONICS CO
1300 E EDINGER AVENUE #D
SANTA ANA, CA 92705
TEL (714)543-5011
FAX (714)543-0553
Email: sales@malltech.com
URL: http://www.malltech.com

Type: Retail/Surplus
Contact: None

This one is useful mainly for the material on their back wall. When they moved into the place, their back wall of the store was lined with these containers (much like a HUGE parts bin). In these containers are all kinds of connectors, components and hardware. They will sell in bulk and give a great price. The more you buy, the better price you get. I've found everything from molex connectors and crystals to atari 2600/5200 cartridge connectors and LED's for less than pennies on the dollar. When you are in the neighborhood (RECOMP, PACIFIC SYSTEMS, ACP SWAPMEET), take a moment to check out ALLTECH.

CONNECT COMP
3016 HALLADAY STREET
SANTA ANA, CA 92705
TEL (714)751-5476
TEL (714)632-5585 EXT 201
Email: ray@connectcomp.net
URL: http://www.connect-comp.com/
EBAY ID: connect-comp

Type: Salvage Yard
Contact: Ray

This place has gone mostly EBAY, but let me tell you about them. They have a wonderful selection of used computer gear and equipment. Check them out and find some great deals!! Here's their self-writeup: "Guaranteed low prices on quality used computers and monitors. We specialize in selling only top brand used computer equipment like Dell, Gateway, Compaq, IBM, Sony, Viewsonic, Mitsubishi, etc" So there you have it. I've found a lot of old Data I/O EPROM programming equipment there as well. I have noticed that they do not sell their entire stock on ebay. They still have a lot of scrap to sort through. The scrap is where I always find my best deals.

PORT CHAIN INDUSTRIES INC
12785 MAGNOLIA AVENUE
RIVERSIDE, CA
TEL (909)279-0819

Type: Salvage Yard
Contact: None

I checked this place out two times right before I quit the entire collecting/buying/selling experience. While I have had no extensive dealings with them, I found them to be a quite surprising source of excess inventory components and scrap computer/equipment deals. They're a little standoff-ish, but they love money just like everyone else, so they'll sell if you tell them exactly what you want and don't waste their time. It's worth a looksie. I know a lot of people who buy and sell monitors with this company. They've been thrilled with Port Chain, so I am lead to believe they're OK to deal with.

INFINITY RE-SALES
(BY APPOINTMENT ONLY)
2936 Lincoln Avenue PMB 13
San Diego, CA 92104
TEL (619)683-7949
Email: jebinf@pacbell.net

Type: Salvage Yard/Swapmeet Sales
Contact: Joshua Bailey

This one is interesting. While I have never made an appointment to see him, I find him over at the ACP swapmeet every other month. I believe he shows up at the TRW swapmeet as well. Both of these swapmeets will be described later - both excellent sources for great deals. I've bought tons of stuff from Joshua. He's really easy to work with and he has great prices. The last deal was a pile of 50 Tektronix P6460 PODS complete with leads and a little over 1500 grabbers for $220. SCORE!!! Ebay selling price on these: $30-$60 each for the PODs, $20-$40 each for the leads. Grabbers sold for $35 per set of 10. $220 in and over $9000 out in a simple deal. I don't think he sells anything on ebay, so his pricing tends to remain very reasonable (read: VERY LOW). Find this guy and tell him what you're looking for. You'll get a wonderful deal. The deals are there, every time I see him.

JK ELECTRONICS
6395 WESTMINSTER BLVD.
WESTMINSTER, CA 92683
TEL (714)890-4001
FAX (714)892-6175
Email: sales@jkelectronics.com
URL: http://jkelectronics.com

Type: Retail/Surplus
Contact: None

This is a retail store located in Westminster, CA. What's cool about this store is that they deal with a small amount of surplus parts and equipment and there's always a treasure to be found. I've picked up everything from IC's for $5 a box, to connectors and switches for about 1/100th of a penny each, to a box of 12 Fluke 9010A Microsystem Troubleshooters complete with dozens of PODS (8080, 6502, 6800, 68000, Z80, 6809) for only $50 for the entire package. At the time, these 9010A's sold for $300-$400 with one or two PODS included. The PODS sold for anywhere between $30-$150 each! Cha-ching!!

When you first walk into the place, it looks like your average electronics store. What you need to look for is the surplus section on your right. Make your way over there and look for the "good stuff". If you don't like the price, walk up with the whole box and do a little wheeling and dealing. For instance, they sold 1MHz, 3.579545MHz (colorburst), 5MHz and 12MHz crystals (new old stock) in small boxes which contained roughly 4000-5000 loose pieces each. Each crystal was marked at $0.25 each. I brought the boxes up to the counter and walked out with them for only $25 a box!! Needless to say, this was a killer deal!

Anyhow, this one is worth a mention because quite frankly, I've made thousands off the items I've bought from this place. It's worth a visit every now and again even though they don't have a huge supply of surplus like the big boys listed above.

ECSC (Electronics and Computers Surplus City)
P.O. BOX 3148
REDONDO BEACH, CA 90277
TEL (800)543-0540
TEL (310)217-8021
FAX (310)217-0950
Email: ecsc@cio.com
URL: http://www.cio.com

Type: Salvage/Surplus/Excess Inventory
Contact: Barry Gott

This place used to be my most favorite salvage yard to visit. In fact, I visited this place for over a decade, finding awesome deals every single time I dropped in on them. They've shut down the yard, but they show up at all of the electronics swapmeets every month. You'll find them at ACP and TRW. They still have a lot of interesting items for sale. If you check out their website, you'll find all sorts of interesting items for decent prices. The real meat of this particular mention is BARRY (yes, a person). He's the owner/operator of ECSC and he's one heck of a cool guy to know. He knows everyone in the business and everything about every company in the business. He's what I like to refer to as the grandfather of electronic surplus. He's been around since the beginning and he's watched all the big guys start from scratch. If you want to know where to find something (and if he doesn't have it), he'll tell you where to find it.

Let me give you some history on this outfit. They used to run a BIG (and I mean, HUGE) salvage yard in Gardena, CA off of Artesia. A picture of the old yard is on their website - boy, it brings back the memories. (sob, sob). Everytime I went to this place, they had junk (and I mean, the good stuff kinda junk) piled 10 to 20ft high everywhere... and this was outside of the building. Inside was an incredible selection, much like a well stocked electronic store, but way better. They had it all. Chips, caps, resistors, meters, motors, diodes, rectifiers, transformers, connectors, wire, switches. Man, they had it all and then some! And none of this was scrap - it was all excess (usually NEW) inventory at rock bottom prices! What the best part was that if you brought out a big load of let's say $25,000 retail value worth of parts, waited to talk to BARRY and get a price from him, you'd walk out with the entire load for maybe $200-$300 at most. It was too easy to spend money here. I still have parts coming out of my ears from this place which I'll probably never use, but who cares. A deal is a deal and this place had the deals like no other.

Back to the yard with the 20ft high loads of junk. I spent a lot of time digging around in the yard. I found all sorts of interesting scrap items that I was always able to turn into profit. I suppose it was more of a field trip for me than anything else but there were some treasures to be found in those piles. I found them, too.

Anyhow, sometime down the road, they either left the building they had or got the boot out of the bulding, I was never too sure on this one. Either way, they still showed up at the swapmeets every month, so I still bought some stuff here and there, but not like when they had the scrap yard. Whenever I hit up the swapmeets, I always make it a point to talk to Barry. He's worth every second of time I've ever spent with him. So, next time you're at ACP, check out the SouthWest corner of the lot and you will find ECSC and probably Barry if you look around. He's the bearded guy with the hat. If he doesn't have a deal for you, he'll tell you who does. Talk to this guy and if he helps you, buy something from him. Hey, he's still got to make a living and information is worth $$$.

UPDATE At the time of the writing of this article, Barry was alive and well. Unfortunately, he has since passed and his kids are now running the business. We're all very sad to see Barry go.

ORVAC ELECTRONICS
1645 E. ORANGETHORPE AVENUE
FULLERTON, CA 92831
TEL (714)871-1020

Type: Retail/Surplus
Contact: None

Orvac is one the of the places I first explored in the 80's. I found this place to be quite exciting at the time. While they are a fully stocking retail store, they also have a surplus section. Yes, it's gotten smaller over the years, but they still have one. They mostly have connectors and switches in the surplus section, but from time to time other obscure items show up like transformers, displays (LCD, LED, etc). I have bought many loads of connectors from these people for less than wholesale over the years. They have been a great backup source since the day I first found out about them. Once upon a time, they used to sell grab-boxes, much like the ones Radio Shack used to sell in the 70's -- but MUCH larger.. and only $1 a box. The amount of goodies was massive. Anyhow, check them out because they're still useful and have the potential to make anyone some money.

SAV-ON ELECTRONICS
13225 HARBOR BLVD
GARDEN GROVE, CA 92843
TEL (714)530-0555

Type: Retail/Surplus
Contact: None

This is another retail location who has a surplus section. What I find unique about this place is the amount of surplus flyback transformers they manage to come up with. They buy from a source (Electronics Warehouse in Riverside - mentioned below) for some of the surplus they sell, sometimes the prices are better than that of Electronics Warehouse. Either way, they have a good selection of vintage parts for less than wholesale. This one rates a 4 out of a 10 on my scale, but it's still useful overall.

FORD ELECTRONICS
8431 COMMONWEALTH AVENUE
BUENA PARK, CA 90621
TEL (714)521-8080
FAX (714)521-8920
Email: sales@fordelectronics.com
URL: http://www.fordelectronics.com

Type: Retail/Surplus
Contact: None

I've been buying from them from these people since the 70's. They have a full retail store intermingled with surplus parts. Just about everything is a surplus part and entitles you to wheel and deal with them. I once picked up a load of roughly 15,000 thousand each of 7 different types of bridge rectifiers. These each sold for $5+ retail at the time, but I paid less than $0.01 per piece. I've been selling these off for $5-$20 each for the last 18 years and I don't see any end to my supply anytime soon! They have a section with old electronic junk, too - I found a few items with Intel 4004 boards inside them - with socketed "gold" C4004 and support chips on each board. I paid $5 per unit and walked away with a smile. There are still deals like this to be had at this place. They always talked to me about their overstocked "warehouse" which I never made the time to make an appointment to visit, but it sure sounds like the place to be. I'm still considering checking this warehouse out someday just out of curiosity (I'd be able to write about it, then). Anyhow, this place has some excellent deals on old parts - they have a BIG chip supply, so ask them if they have what you're looking for - it can't hurt.

BALL ELECTRONICS
2960 W. BALL ROAD
ANAHEIM, CA 92804
TEL (714)828-1310

Type: Retail/Surplus
Contact: Larry

This one is a mom and pop operation which has been around longer than most electronic stores. I have mixed feelings about this place, but they're worth the mention. They have a surplus section which takes up a good portion of their store - in this surplus section, they have connectors, caps, diodes, switches, displays, sockets, scrap circuit boards, old junker equipment and hardware parts. It's really kind of interesting. The guy who runs the place is a bit moody and his prices fluctuate ... in fact, he's downright difficult to hagle with, but I find that persistence prevails with him. Just keep on top of it and he'll cave in....eventually. I once bought a large pile of circuit boards (roughly 150 of them) from this place. Each board was riddled with piles of socketed logic, gold plated CPU chips, and RAM chips (4116, 2115, 6116, etc). I paid $0.50 per pound and walked away with another excellent deal. No need to haggle with him on this one. He said the price and I paid. I had no idea what I really stumbled upon until I looked everything over a week later. Come to find out, I had picked up a pile of Ohio Scientific 500 and 600 series boards. You know, vintage computer boards which just happened to be highly collectable. Score! They have a somewhat decent selection of old chips and vacuum tubes. Check them out.

THE BEGINNERS GUIDE TO SCANNING

By radio_phreak

Right I am back by popular demand with a segment on radio scanning, so I thought how about I write you all a guide with some pointers? I am everyday discovering new frequency's in my local area (I live in south east England). With this article I am going to show you how I personally find frequency's. You might have your own way that you find perfectly fine and by all means don't listen to me that's fine but this works for me and I would like to share it with you. In this article I will give you some small pointers on how to discover frequency's and traffic analysis. First a little explanation as to what traffic analysis is. It sounds pretty cool doesn't it? (well it does to me) but all it is, is at the most basic level is leaving your scanner locked on 1 frequency to determine what is in use on the said frequency. Some people prefer to go further in depth and go the whole wack with spectrum analyzer plots and direction finding, my solution is very simple and 1 that everyone is capable of using again you may think my method is no good and may want to develop your own method and that's fine as well.

How to discover the frequency's

First off you need to take a couple of things into account:

1. What exactly are you looking for? take for example airplanes, you know that it falls between 108-137MHz (AM) so you know to search between them (Dont forget which mode it is as well listening to AM in NFM mode sounds weird!)
2. The location, say if you are looking for a mall security frequency, there is no point in trying to listen to a frequency 70 miles away when it's on UHF
3. What time do they operate from? Taxi's are 24/7 however interstore comms will stop at the end of the business day or it could even be a security firm or nightclub that only operate at night times
4. Are you suitably equipped? Your scanner might only cover 25 - 173 MHz and the frequency you are searching for may be at 201MHz for example, so your scanner is next to useless. Are you using the right type of aerial? if not you may want to upgrade it, the aerial that comes with your scanner is usually okish but they aren't great think about purchasing or home brewing a Dipole or Discone
5. Also bear in mind that some frequency's are not meant to be shared, say for example cash delivery guards because by making that kind of thing public knowledge you may well have aided a gang in planning a robbery
6. Don't make it to widely known that you are a scanner I refer you to my previous article, if you have a radio license you have more than enough excuse to be carrying all sorts of radio telephony equipment. If not you may find yourself being asked some awkward questions.
7. As above, be discreet don't walk up to people and ask them what frequency they are on and don't be seen to be taking to much interest in people's radio equipment it seems to make them nervous
8. Consider investing in a close call™ or signal stalker™ equipped scanner this basically means you can sit there and leave the close call running, any transmissions that pop-up your scanner will automatically tune into it and you can either discard or take note of the frequency, they don't usually cost anymore than a frequency counter and the bonus side of it is that you can actually listen to the frequency you have found automatically, excellent for long distance road trips.
9. If you are operating from home, make your lair/pit/hole/home/wherever as comfortable as possible. Consider getting in a nice comfy chair, cheap food (Gloop) and something to entertain yourself while you are waiting for something to pop up. You may have to wait a while when you are scanning, just because you aren't hearing or finding any new frequency's doesn't mean that they are not there, just means they aren't transmitting
10. Be prepared to share your finding's you will find that once you have shared others will be more than willing to share back (remember what I said about something's are not to be shared though)

Traffic Analysis Tips

1. Find the frequency you wish to find out more about in this list I will be referring to my local Port Control Frequency
2. First of all determine who is in control of the said frequency is there a clear call sign that says anything like control?
3. What call signs are in use on the frequency? To call the control at the port you call "Ramsgate Port Control" ships usually identify themselves by there name, but there is also an ships international call-sign so that all country's can identify ships uniquely (because sometimes ships names tend to be repeated amongst others)
4. What are the procedures in use on the frequency, say for example a security company may try and task CCTV to keep an eye on someone, in the local port to leave the port they say "Dover Port control permission to leave to the harbor) determine procedures once a call has been put out
5. What CCTSS tones are being used? Are there alert tones that can be sent out if an officer or a ship is in trouble?
6. What mode are is the user using? NFM,WFM,AM,SSB,USB,LSB,DFM,ATV,SSTV,PSK31,RTTY?
7. Other things you may want to keep a track of are the times and the duration of the call, this can help determine internal procedures such as perimeter patrol times, CCTV scans, shift change etc
8. Consider purchasing a hardware based or download a software based spectrum analyzer this can help you in determining the frequency, any tones that may come up it can also help you determine what (if any) type of data is being used
9. Don't be afraid to go online and ask for help because 9 times out of 10 you will usually find someone to help you and if they don't answer you or flame you then you are either asking the wrong people or they don't know themselves and are trying to deflect any attention you have aimed at them
10. If you have access to an S-Meter you can also determine signal strength, these are available from ham fests or retail outlets.

An example Traffic Analysis log may look something like this (it depends on your preference):

Frequency	Mode	Tone	Known User	Date	Time	Notes
156.7000	NFM	None	Ramsgate Port Control	08/25/2006	16:34:06	Ferry to Ramsgate Port Control:R'Gate Port Control ****spur Permission to leave
156.7000	NFM	None	Ramsgate Port Control	08/25/2006	16:34:47	Ramsgate Port Control to Ferry: Permission to leave"
156.7000	NFM	None	Ramsgate Port Control	08/25/2006	16:45:02	Ferry to Ramsgate Port Control: "*****spur clear of the channel good evening and good watch"

You get the idea anyway. It can come in handy to aid in the determination of traffic on a certain frequency (i.e. 1 that rarely transmits if at all!)

Port of Ramsgate

Also don't forget as well there are some things that are not meant to be shared or mentioned (if listening to a frequency in use by what seems to be intelligence or military) and some are meant to be shared. So there you have there are a few tips to get you started. I hope that this kind of information helps you. Also don't forget most information about most thing's can be found on the net with a little bit of research as many a good phreak/hacker knows research is very important so consider buying literature on radio's and antenna's. Also keep an eye out for my homebrew Sat TV dish hack in which I will show you how to convert an old Sat TV dish into something usable with your 802.11 network or Bluetooth projects. I may also do some equipment reviews in the future and eventually talk further about war tracking (the process of tracking and listening to satellites) I will also talk about the INMARSAT's plans to abandon there constellation of INMARSAT analogue satellite's and what that means for us in the global phreak/hacker community (basically that means there's a freebie for us all to use!)

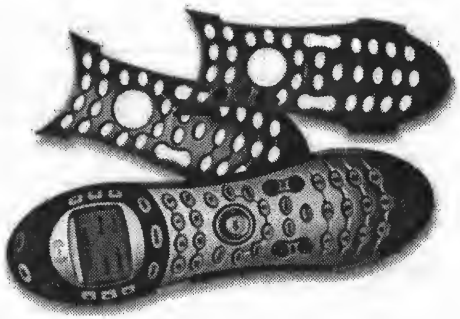
Signing off

Radio_phreak

Logitech Harmony Remote Review

Written by: TheInstallGuy

Today, I am going to give my personal review of the Logitech Harmony 676 Remote. I just purchased one the other day, and am enjoying it so much, I figured I would share my experiences with it. The Harmony 676 is the middle to high end remote. At the time of this writing, the cost was $149.00 CDN. Currently, the Logitech web site is selling it for about $229.00 CDN, which is a little odd, but I will right it off to the web site not being updated. That being said, let's get started.



How It Works: Quick and easy set-up by connecting the Harmony Remote to your home computer via USB.

Create an account on HarmonyRemote.com, and follow step-by-step instructions to tell us about your configuration. It's as easy as picking your components from lists and supplying us with the component's model number. Download the configuration to your Harmony Remote by attaching it to your Windows or Mac PC via the supplied USB cable.

Once your Harmony Remote is configured, it can control your entire home theater system with one button press! Using Activity buttons labeled "Watch a Movie", "Watch TV", "Listen to Music" and "More Activities", your Harmony Remote can send all the right commands to your entertainment system without requiring you to program a macro.

Controls all brands and device types
The Harmony Remote has access to the largest online database of devices. This means that it will support all brands of Televisions, Projectors, Monitors, Amplifiers, Stereo Receivers, Audio/Video Switches, Channel Decoders, Cable Boxes, Satellites, Digital Set Top Boxes, Video Recorders, VCRs, PVRs, TV/VCR Combos, DVDs, DVD Recorders, Laserdisc Players, DVD/VCR Combos, CD Players, CD Jukeboxes, Digital Music Servers, Game Consoles, Mini Systems, Computers, Microsoft Windows XP Media Center Edition PC, Laptops, Tape Decks, Light Controllers, Minidisc Players, DATs and more! There is even a specific activity for the Harmony Remote that integrates your Microsoft Windows XP Media Center Edition PC with your entire entertainment system.

Packaging: Enclosed in a nicely put together package is the following:

- Harmony® 676 remote control
- 3 changeable faceplates (Metallic Blue, Metallic Red, and Silver)
- USB cable
- Installation CD
- Installation guide
- 4 AAA batteries (DuracellJ)
- Limited 1 year repair/exchange warranty from date of purchase

You can be guaranteed to receive everything in the package. There is no way anything can be removed from the plastic tray insert. This tray holds all components and is sealed on all four sides. If it has been cut open and put back together, you will know. All in all the packaging is good. It did take me 5 minutes to get into it, but I knew everything was there.

Setup: The instruction manual was pretty well laid out. The instructions were simple to follow and there was even a small chart included that allowed you to write down all of your devices before you start programming the remote.

For the sake of this article, I decided to follow the directions to the letter in order to deliver a fair analysis of the process. From the start, everything went as expected. Put batteries in the remote and locate devices you wish to program into the remote. There are clear examples of what info is needed from any device you may want to use and the chart is large enough to actually read what you write down.

To the computer! At this point, the rest of the configuration takes place on your computer. My installation was on a Windows XP machine, but Mac is also supported from the same CD.

Minimum Requirements: Win 98SE/ME/2K/XP, IE 4.0 or better 10MB HDD space, and an internet connection. Mac: OSX Only, Safari 1.0 or better, 10MB HDD Space, and an internet connection. The program is located here: cd/ Harmony Remote/Software.mpkg

The first difference I noticed was that the instructions asked me to plug the USB cable into the remote and the PC before inserting the CD. Usually we are confronted with the oversized yellow sticker "DO NOT plug in device until software is installed.....you n00b". However, I said I would follow the instructions. To my surprise, no new found hardware wizard.....sweet! The device was just installed as stated in the manual, as a Human Interface Device. I imagine Windows 98 and ME users would be forced to dig their Windows CD's out of the closet.

Ok, so I am on page 6 of the instruction manual and all is going well. At this point, I am asked to insert the disk into my PC. Now, the reason I even bring up this point is I am expecting to be ravaged by pop-ups that state that "this software has not passed Windows logo testing". To my surprise, I receive no such warning. For those of you counting, that's twice my assumptions have been wrong. Kudos to Logitech so far for a well put together installation package.

The software did install without issue in about 25 seconds. After the installation completed, the instructions state that the computer may or may not reboot. Mine didn't. Instead, I was immediately redirected to a web page that wanted me to upgrade the software I had just installed. In addition, another window opened and wanted me to start the configuration process. From here the instruction manual is useless and a little confusion ensues.

Instinctively, I want to upgrade the software first. Clicking the upgrade button opens a third window identical to the configuration page that is already open. Ok, I guess we are configuring the remote first. The online configuration wizard is nicely laid out and easy to read. No sooner than I click next, the upgrade page shows up. The instructions state that the program will be upgraded and the remote will be flashed with a new firmware upgrade. The upgrade started with no issues, but 5 minutes in, the installer is frozen and the computer is locking up ...REBOOT!

Strangely enough, I feel I am in a familiar place. New software, new product, Windows crashes, but in the interest of a fair trial, we will move on and try again. Looking back in the instruction manual for the reboot after installation part, I found the link used to gain access to the Harmony Remote page; http://www.harmonyremote.com. Upon my second visit to this site, I am prompted to create an account. Now, I do remember seeing this page earlier, but was pushed passed it to upgrade he software and firmware. The account page is pretty straight forward and allows you to leave out certain personal information that you may not want to share (Nice to see our privacy is important to some companies). At the end of the form is the always present "Would you like to receive special offers from so and so", No spam for me, thanks!

After this point, I was again prompted to upgrade the software and firmware. This time the upgrade went off without a problem. I had the current software and firmware downloaded and installed in about 3 minutes. From here, I was led to a page that asked for all my devices I wished to use. I entered the information exactly as it was on each device (I did use caps and dashes where needed), clicked next and moved on. The software had recognized every device as I had entered except for my TV set top box (Motorola RG-2400). At this point, I was asked to retrieve the remote and place it 1-2 inches away from the bottom of the Harmony remote. After pressing a few buttons when instructed, I think there was 4 buttons to press), the Harmony remote had learned every facet of my Motorola remote…….again, Sweet!

From here, all that was left was to answer simple questions about how I used certain devices and what channels and receiver settings I used. Lastly, I was told to press the save button and test the remote with all devices. Everything worked perfectly! I did not have to perform any tweaks or reprogram any devices back into the remote. It just worked as it was supposed to.

Life Since Setup: It has been about a week since the initial setup of the Harmony Remote and all is well. There have been no instances of pulling out an old remote looking for a certain feature that is not on the new remote. In fact, I can even program all of my Dolby and FX features from my receiver on the LCD of the Harmony Remote. At this point and time, I can honestly say that I will never go back to a multiple remote situation.

The remote its self has proven to be durable as well. There have been a few occasions where it has hit the floor with a good thump and has shown no signs of damage at all. The LCD screen is bright and easy to read. There are also 6 buttons on either side of the screen that allow for more advanced settings to be changed. I was also impressed with the way the lettering on the buttons is done. It appears that they are all screened below the one that is in constant contact with your fingers. If I am correct, I would tend to believe that the numbers and letters will not fade on the remote, increasing its longevity.

Conclusion: My biggest problem with the Harmony 676 Remote is the software installation. Don't get me wrong, I do understand the need for updates and fixes. I would hope that newer software will be included in future packaging. In the very least, I believe Logitech should refine the web interface to not have 2-3 windows open up with different instructions. To the average user, this creates a mass amount of confusion.

All in all, I believe this unit to be an incredible addition to any home theatre user, regardless of the price. I give it a 9 out of 10.

Pro's: Great feel and look – not heavy or bulky
Easy to read buttons and the backlighting (glow feature) covers all buttons
Over 80,000 IR Codes and a seemingly unending list of devices
One touch control to turn on all devices relating to a task

Cons: Flakey installation software (at least for now)
Expensive

References:
How it works section – content by Logitech http://www.harmonyremote.com
Direct link to Harmony 676 - http://www.logitech.com/index.cfm/products/detailsharmony/CA/EN,CRID=2084,CONTENTID=9511

Picture is courtesy of – http://www.harmonyremote.com

The Black Market

URBAN EXPLORATION! Phone obsessions! Pointless conversation! And a slight chance of hacking! It's Doug TV baby http://www.dougtv.org

LOCKPICKING101.COM Open forum discussion to educate yourself and others about lock picking and lock security.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles will come from newspapers, magazines, online resources, and more. For more information: http://www.c4i.org/isn.html

I'M RAFFLING my original APPLE-1 computer I have no use for it anymore so I'm giving any one who wants a chance on owning a piece of history all I ask is for a one paragraph letter telling me why you would want my computer, and $2.00 cash or money order to: MY RAFFEL, 567 W. channel Isl. Blvd., Port Hueneme CA, 91341 suite 416

HACKER STICKERS Geeks, Coders and Hackers get your stickers, shirts, hardware and caffeine from www.hackerstickers.com

TRUE TAMPER-PROOF Security Screw Removal Bits. The super torx kit includes: T-10, T-15, T-20 & T-25. Complete set for $19.60. TOCOM 5503 bit $8.95. TOCOM 5507 bit $19.95. Zenith PM/PZ-1 bit $10.95. Jerrold Starcom bit $19.95. Pioneer (oval) bit $23.95. Oak Sigma (oval) bit $23.95. Security Screws available. Tamper-Bit Supply Co. (310)866-7125.

HIGH-TECH security/survival books/manuals: Computers, Internet, Phones, Energy, Physical Survival, Financial, Law, Medical/Radionics, Mind Control, Weird/Paranormal. Free Online Catalog at: Consumertronics.net (PO 23097, ABQ, NM 87192), or $3 hardcopy (USA/Canada, $7 foreign). See display.

HOME AUTOMATION. Become a dealer in this fast growing field. Free information. (800)838-4051.

TIRED OF SA TEST KITS with marginal or inconsistent performance? 21st Century Electronics and Repair guarantees peak performance with 40-pin processor kits. New, more flexible program with additional features puts others to shame. Price $49 each or 5 for $233. 1st time offered. (404)448-1396

FEDERAL FREQUENCY DIRECTORY! Kneitel's "Top Secret" registry of government frequencies, New 8th edition. 268 pages! FBI, DEA, Customs, Secret Service, BATF, Immigration, Border Patrol, IRS, FCC, State Dept., Treasury, CIA, etc. & surveillance, bugs, bumper beepers, worldwide US military, 225 to 400 Mhz UHF aero band, Canadian listings, & more! Ultimate "insider's" directory! Standard reference of law enforcement, news media, private security, communications industry & scanner owners. $21.95 + $4.00 shipping ($5.00 to Canada). NY State residents add $2.21 tax. CRB Research Books, Box 56BL, Commack, NY 11725. Visa/MC welcome. Phone orders (516) 543-9169 weekdays (except Wednesday) 10 to 2 Eastern.

TOP SECRET SPY DEVICES Home of the Worlds' Smallest Digital Voice Recorders and Spy Cameras. We stock many items including: Transmitters, Bug Detectors, Audio Jammers, Telephone Recorders, Lock Picks, Voice Changers, Keystroke Loggers. www.spydevicecentral.com (305)418-7510

HACKERS '95 THE VIDEO by Phon-E & R.F. Burns: See what you missed at Defcon III and Summercon 95! Plus, our trip to Area 51 and coverage of the "CyberSnare" Secret Service BUSTS. Elec Cntr Measures, HERF, crypto, and more! Interviews with Eric BlookAxe, Emmanuel, and others. VHS 90 min. Only $25 - distributed by Custom Video 908-842-6378.

EUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge mail-order source for over 1,000 titles. Beautifully illustrated 128-page catalog includes: alternative/fringe science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3.00 to Xines, Box 26LB, 1226-A Calle de Comercio, Santa Fe, NM 87505.

6.500 MHZ CRYSTALS $4 a piece, 50 for $115, 100 for $200. Add $3.00 for shipping. Send checks to C. Wilson, P. O. Box 54348 Philadelphia, PA 19105-4348

COIN-OP VIDEO ARCADE GAMES. Parts, boards, and empty cabinets available for your projects. Cabinets available for $75. C.J. Stafford, (301)419-3189.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes catalogs of selected (no junk) shareware and restricted books. Send $1.00 for S.25 disk, $1.50 for 3.5, plus two stamps, to: MENTOR PUBLICATIONS, Box 1549-W, Asbury Park NJ 07712

ANARCHY ONLINE A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted E-mail/file exchange. WWW: hhtp://anarchy-online.com Telnet: anarchy-online.com Modem: 214-289-8328

HACK THE PLANET A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Hand-scanned 99XX exchanges in 516 AC. Included may be data kit modem numbers, WFA/FA, SSCU, TSAC(SCC), CO#'s, etc. Send $2.00 check or money order payable to CASH and specify exchange. "MCI-Style" Phone Patrol hats are now available! Just $18 check or money order payable to CASH. 2447 5th Ave, East Meadow, NY 11554.

ATTENTION HACKERS & PHREAKERS. For a catalog of plans, kits & assembled electronic "TOOLS" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTER SURVEILLANCE, CABLE DESCRAMBLERS & many other HARD-TO-FIND equipment at LOW PRICES. Send $1.00 to M. Smith-02, P.O. Box 371, Cedar Grove, NJ 07009

VOICE CHANGING ACCESSORY. Digital voice changing: male to female, female to male, adult to child, child to adult. Use with any modular phone. 16 levels of voice masking. Connects between handset and phone. STOP THOSE ANNOYING TELEPHONE CALLS! Sound older and tougher when you want to. Not a kit. Fully assembled. Use with single or multi-line phones. 30-day refund policy. Ask for free catalog of our products. VISA/MC ok. Xandi Electronics. 1270 E. Broadway, Tempe AZ 85282-5140. Toll Free order line: (800)336-7389. Technical Support: (602) 894-0992

MAGENCODERS.COM Manufacturer of the World's Smallest Portable Magnetic Card Reader & Point of Sale Data Loggers. We also have Magnetic Stripe Reader/Writers, Smart Card Loaders & Copiers, etc... (407)540-9470

UNDETECTABLE VIRUSES. Full source for five viruses which can automatically knock down DOS & windows (3.1) operating systems at the victim's command. Easily loaded, recurrently destructive and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well-written documentation and live antidote programs are included. Priced for sharing, not for making a ridiculous profit. $10.00 (complete) on six 1.44MB, 3.5" floppy discs. Money orders and checks accepted. No live viruses provided! Do NOT ask. Satisfaction guaranteed or you have a bad attitude! The Omega Man. 8102 Furness Cove, Austin, TX 78753

NO SOUND ON PREMIUM CHANNELS? It will happen sooner or later on your Jerrold DPBB-7 Impulse. Ask Manhatten! Soundboard brings the sound back. Best sound fix on the market. Easy to install soundboard $24.95. Easy to build soundboard schematic, parts list and common chip number $34.95. Send us your unit and we will install the soundboard for $59.95. SOUNDMAN, 132 North Jardin St., Shenandoah, PA 17976. (717) 462-1134.

SINGLE DUPLICATION OF CD-ROMS Send your CD and $25 and you will receive your CD and an exact copy. Want more than one copy? Send a additional $15 for each duplicate. Make checks or money orders Payable to/Mail to: Knoggin, 582 Merket Street Suite 616, San Francisco, CA 94114

CB RADIO HACKERS GUIDE! New! Big 150 pages; pictorials, diagrams, text. Peaking, tweaking and modifying 200 AM and SSB CB radios. Improved performance, extra capabilities! Which screws to turn, which wires to cut, what components to add: Cobra, Courier, GE, Midland, Realistic, SBE, Sears, Uniden/President. $18.95 + $4 S&H ($5 Canada.) NY State residents add $1.96 tax. CRB research, Box 56BL, Commack, NY 11725. Visa/MC accepted. Phone order M-Tu-Th-F, 10 to 2 Eastern time. (516) 543-9169.

NULL MODEMS - Download laptop: or upload to your pc the easy way! w/ direct connect, or (DOS 6.1) Customized setup, no bulky adapters, MAC or IBM compatibles. Send $18.95 for 6ft cable, specify 25 or 9db ends, custom ok. Instructions included. P.O. Box 431 Pleasanton, CA 94566 (510)485-1589

A TO Z OF CELLULAR PROGRAMMING. Programming instructions on over 300 phones in a software database. Also back door and test mode access instructions for all the popular models; manufacturer's contacts, system select, lock/unlock info. Just $59.95. Orders only: (800)457-4556, inquiries: (714)643-8426. C.G.C.

GAMBLING MACHINE JACKPOTTERS We offer a complete range of gambling products designed to cheat gambling machines as well as other games. Our products are designed to demonstrate to gambling machine owners the vulnerabilities of their machines. Our product line consists of Gambling Machine Jackpotters, Emptiers, Credit Adding Devices, Bill Acceptor Defeats and Black Jack Card Counting Devices. Please visit www.jackpotters.com

KEYSTROKEGRABBERS.COM Manufacturer of discreet keyboard logging hardware. Our devices capture ALL keystrokes on a computer including user name and password. PARENTS---Monitor your child's internet, e-mail, instant messaging and chat room activity. EMPLOYERS---Monitor employee computer usage compliance. Employees will spend less time browsing the internet and sending e-mails if they are being monitored. EXECUTIVES & SYSTEM ADMINS---detect any unauthorized access of your PC. If someone uses your computer after hours, you will know. (305)418-7510

HACKING, PHREAKING, computer security and education on the First Tuesday of every month in the Detroit area. Meeting is at 7pm at Xehdo's cafe in Ferndale. Bring your open mind and positive attitude.

I WANT TO OFFER my playstation 2 game burning service. Any game that you would like for a back-up or just for fun. Or maybe that Japanese game that just won't be out in the United states for a few months.. I have bundles that you can choose from if you want handfulls depending how much you order. the games are $25 each !PLEASE NOTE THAT YOUR PLAYSTATION 2 NEEDS TO BE MODDED I ALSO HAVE THAT SERVICE BUT YOU CAN ALSO GOOGLE SEARCH FOR PREMODDED SYSTEMS TO BUY. EMAIL IF YOU HAVE ANY QUESTIONS AT ALL.

ACCUSED OF A COMPUTER RELATED CRIMINAL OFFENSE IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in the defense of alleged cybercriminals, including but not limited to, hackers, crackers, and phreaks. Not a former prosecutor seeking to convince defendants to plead guilty, but an idealistic constitutional and criminal defense attorney who helped secure a total dismissal of all charges in Los Angeles Superior Court for Kevin Mitnick, who was falsely charged with committing computer-related felonies in a case with $1 million bail. Please contact Omar Figueroa, Esq., at (415) 986-5591, at omar@aya.yale.edu or omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation for Blacklisted 411 readers. (Also specializing in medical marijuana and cannabis cultivation cases.) All consultations are strictly confidential and protected by the attorney-client privilege.

HACKERSHOMEPAGE.COM - Your source for Keyboard Loggers, Gambling Devices, Magnetic Stripe Reader/Writers, Vending Machine Defeaters, Satellite TV Equipment, Lockpicks, etc...(407)650-2830

I-HACKED.COM is a hardware hacking based website and it currently looking for articles! Membership is limited to contributing members, so come and share your knowledge with other hackers around the world. Topics we are currently looking for include: DVD "Dual-Layer" Firmware hacks, CD-RW / DVD+/- Speed Hacks, Video Card Hacks, Motherboard Hacks, IDE Card / Raid Hacks, Xbox Hacks, Playstation Hacks, cell phone tricks, or anything else you might have. Check us out @ http://www.i-hacked.com

ADD A CONVERSATIONAL USER INTERFACE to your web site or Windows-based software applications with Foxee™, the friendly interactive arctic blue fox agent character! In the real world not everyone who navigates your web site or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net!

DO YOU WANT MORE underground information? Are you ready to go to a whole new level of knowledge? Then you need to check out "Binary Revolution" magazine.
 Is a printed hacking magazine put out by the DDP that covers hacking, phreaking, and other assorted topics from the computer underground. For more information on the magazine, forums, HackRadio, HackTV, or any of our other numerous projects, come to www.binrev.com and join the revolution. "THE REVOLUTION WILL BE DIGITIZED."

TUNE IN TO CYBER LINE RADIO on the internet, on the USA Radio network. We can be heard Saturday Evenings 9:00 pm to 12:00 am (Central). Heard Exclusively On The USA Radio Network & Via The Internet! We discuss Technology, Space, Hacking, Linux and more. For more details meet us at www.cyber-line.com.

BLACKLISTED MEETINGS will begin in Greece as the new year arrives, They will be held every 3rd saturday of the month and they will begin at 7pm. Meeting point will be the centre of Athens at the metro station Panepistimio by the fountains. Also check the webpage www.blacklisted411.gr.

A+ CERTIFIED TECHNICIAN offering cheap repairs in Louisville Area. Will make house calls or take home with me. I do everything from virus and spyware removal to networking. Send an email to alanb6100@gmail.com with your name and phone number as well as a description of the problem. Also I have Gmail invites available for a reasonable price. Louisville area only unless you want to Western Union me some money! Thanks!

SELLING USED HIRSCH SCRAMBLEPADS that relail new for around 500$ for your best offer! They are for very high security places, every time you press the START button on the keypad it randomizes the digits so that any onlookers cannot find a pattern in the digits you press. Also, you cannot see the numbers from the side, so for anyone to see your code they would have to be directly behind you. Email me for more information. guiltyspark414@netscape.net

WANTED: FEATURE FILM JUNKIE who can access up-to-date FAX numbers for hot agents and/or producers & directors. My objective: to bring to their attention my action-thriller script. Can pay by the hour. (909)275-9101

HI, MY NAME IS RICK. Me and my friend Rob where looking for a low cost rackmount server one day to use for a web and mail server that we could have racked at a local datacenter, Not finding anything real cheap we decided to start our own company building fast cheap servers for you also. www.cheap1u.com was born. Mention this ad and get 10% off any server order. Also since I am the owner, if you mention this ad buy 10 servers and I will throw in the 10th server for free!

MONTHLY MEETINGS

Interested in meeting up with some of the Blacklisted! 411 readers? We will list all hacker meeting information that is provided to us. We will list "Blacklisted! 411" only meetings as well as "independent" meetings open to all.

California

(949 Area Code) - Irvine

Extreme Pizza - 14141 Jeffrey Road, Irvine, Ca. 92714 - Meeting is not Blacklisted! 411 specific. The meeting date may change from month to month. For specifics, check here: www.irvineunderground.org

Hosted by: Freaky

Colorado

(719 Area Code) - Colorado Springs

DC719 - Hack the Rockies. Meetings held on the 3rd Sat. of every month. 8pm-11pm @ Xtreme Online, 3924 Palmer Park BLVD

Hosted by: DC719 POC: h3adrush

(303 Area Code) - Centennial

We meet the first Friday and third of every month at 5:00pm at the Borders café on Parker in Arapahoe Crossings.

Hosted by: Ringo

Florida

(407 Area Code) - Orlando

The computer room in the Grand Reserve Apts. at Maitland Park

Last Friday of the month, 12:00pm - 1:30pm

Hosted by: Whisper

Georgia

(678/770/404 Area Codes) - Duluth

Meetings are the first and third Tuesday of every month, in the cafe of Frys Electronics. They start at 6:30 until we get kicked out, and then continue elsewhere. Visit our site at www.HackDuluth.org and sign up on the forums to receive emails about the group.

Hosted by: P(?)NYB(?)Y

Illinois

(217 Area Code) - Urbana

Espresso Royale Caffe. 1117 W. Oregon St., Urbana, IL 61801. At the corner of Goodwin and Oregon, across the street from the Krannert Center for the Performing Arts. Every second Friday of the month, 8 PM

Hosted by: r3tic3nt (r3tic3nt@gmail.com)

Iowa

(515 Area Code) - Ames

ISU Memorial Union Food Court by the payphone. First Friday of each month, from 5:00pm onward.

Hosted by: Omikron

Minnesota

(612 Area Code) - Minneapolis

Spyhouse coffee shot at the corner of 25th South and Nicollet Ave. Look for the Blacklisted! 411 magz on the table.

Last Friday of the month, 5:00pm - 8:00pm

Hosted by: Thea DeSilva

New Mexico

(505 Area Code) - Albuquerque

Winrock Mall - Louisiana at I40, food court, east side doors under the security camera dome.

First Friday of the month, 5:30pm - 9:00pm

Hosted by: Mr. Menning

Texas

(713 Area Code) - Houston

In front of Rocfish on Westheimer/Kirkwood. Last Sunday of every month, 7:00pm till close.

Hosted by: MuertoChongo

(915/325 Area Codes) - Blackwell

John's Detectors, 501 W. Main St. Third Friday of every month. 7:00pm until...? For more information, visit our site at www.johnsdetectors.com

Hosted by: Wirechief

Wyoming

(307 Area Code) - Rock Springs/Green River

White Mountain Mall—Sage Creek Bagels. The last Friday or every month from 6:30pm until 9:30pm.

Hosted by: Phreaky

Mexico

(666 Area Code) - Tijuana, B.C.

Café Internet, Calle 12, Felix M. Gomez #844, Col. Libertad. In back room by payphone. First Friday of the month, 5:00pm to 8:00pm

Hosted by: Tom

YOUR MEETING HERE

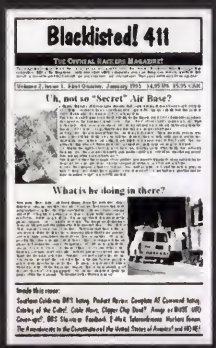
Start up your own meeting and enjoy the benefits! Contact us right away!!

meetings@blacklisted411.net

History Of Blacklisted 411

Started as one of the first disk based hacker magazines in 1983, Blacklisted! 411 has evolved into one of the most widely distributed hacker magazines to date. Since its creation, the staff at Blacklisted! 411 have strived to publish original and controversial articles on a variety of subjects. With the beginning of 2006, Blacklisted! 411 will present new ideas and concepts for the entertainment and education of the security/hacking community. Shown below are some cover shots of past issues ranging from 1994 to 2005.

1994



1995

1996

1997

1998

2003

2004

2005

Blacklisted 411 the Magazine
P.O. Box 2506
Cypress, CA 90630